Planning and Evaluation of Information Security Investments

Dissertation zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

eingereicht an der Fakultät für Wirtschaftswissenschaften der Universität Regensburg

vorgelegt von: Eva Szubartowicz

Berichterstatter: Prof. Dr. Guido Schryen, Prof. Dr. Günther Pernul

Tag der Disputation: 26. Juli 2018

University of Regensburg
Faculty of Business, Economics, and Management Information Systems
Department of Management Information Systems

Dissertation

Planning and Evaluation of Information Security Investments

submitted by
Eva Szubartowicz M.Sc.
to
the Faculty of Business, Economics, and Management Information Systems
of the University of Regensburg
for the Degree of
Doctor rerum politicarum
in
Management Information Systems

Supervisors:
Prof. Dr. Guido Schryen
Prof. Dr. Günther Pernul

Regensburg, April 13, 2018

To my parents Caroline and Maximilian Weishäupl

Preface

This dissertation is submitted for the degree of Doctor rerum politicarum at the University of Regensburg. The research described herein was conducted under the supervision of Prof. Dr. Guido Schryen, between August 2014 and December 2017.

This research was supported by the *Bavarian State Ministry for Education, Science and the Arts* as part of the FORSEC research association (https://www.bayforsec.de).

I would like to thank Prof. Dr. Guido Schryen for his valuable support and enthusiasm, my second supervisor Prof. Dr. Günther Pernul, who also provided advice and feedback and my colleagues Mr. Gerhard Rauchecker, Mr. Gerit Wagner and Mr. Emrah Yasasin each of whom has provided patient help and friendship throughout the research process.

Finally, I would like to take this opportunity to express my gratitude to my family for their love, encouragement and support throughout my entire course of studies.

Regensburg, April 13, 2018 *Eva Szubartowicz*

Table of Contents

Part I

Dissertation Outline

1

Introduction

> *"Today information security is shifting from what is technically possible to what is economically efficient."* (Su, 2006, p. 4)

This thesis provides a theory-based understanding of information security investments within organizations concentrating on organizational planning and evaluation of information security investments. The underlying framework is the *Cyber Security Investment Framework* of Rowe and Gallaher (2006). This work is structured as follows: In the remaining of Part I, the dissertation is motivated and the theory to frame this research is described in detail. Subsequently, in Part II, the publications which comprise this thesis are presented. Finally, in Part III, the findings of this dissertation are discussed.

1.1 Motivation

As successful organizations nowadays rely on information technology for every aspect of their business (Kankanhalli et al., 2003), information technology has become of crucial importance for them (Ernest Chang and Ho, 2006). With cyber security threats taking on new forms and methods, the need to secure firm's systems, data and processes against misuse and attacks is of vital importance (Ernest Chang and Ho, 2006). Successful attacks can result in the disruption of production and processes or data theft, which cause economic damage, including losses in productivity and revenue (Bandyopadhyay et al., 2009). Besides actual and potential financial losses, other negative consequences of information security incidents include negative publicity, competitive disadvantage, and even reduced organizational viability (Kankanhalli et al., 2003). According to Forbes, worldwide costs of data breaches will reach $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015 (Forbes, Inc., 2016). These figures indicate the necessity of information security[1] to protect firms' business operations against internal and external threats (Anderson and Choobineh, 2008; Hall et al., 2011). The prevention of such threats causing security

[1] Information security is defined as *"the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit"* (Spagnoletti and Resca, 2008).

incidents is achieved with protecting organizations' resources through implementing different information security measures (Van Niekerk, 2010). Accordingly, in order to protect the confidentiality, integrity, and availability of their systems, firms invest heavily in information security measures (Gupta, 2008): Gartner predicts information security spending to reach $93 billion in 2018 (Gartner, Inc., 2017). Organizations' information security spending mainly concentrates on software such as anti-virus programs, firewalls, encryption techniques, intrusion detection and prevention systems, automated data backup, or hardware devices (Gordon and Loeb, 2002b).

Information security is a challenging and versatile research field (Spagnoletti and Resca, 2008): With firms spending billions of dollars on information security measures yearly, information security investment has become an extensive area of research (Huang et al., 2006). Various aspects of information security have been researched in detail but most research attention has been paid to the technical side (Ernest Chang and Ho, 2006), e.g., focusing on encryption techniques, access control, or firewalls (Anderson, 1972; Cavusoglu et al., 2009, 2005; Debar and Viinikka, 2005). Next to technical aspects, human factors are included for a *"comprehensive integrated overview"* (Werlinger et al., 2009) to study the behaviour of firm employees or attackers in detail (Kraemer et al., 2009; Kraemer and Carayon, 2007; Safa et al., 2016; Glaspie and Karwowski, 2017).

Concentrating on firms' investments in information security, I discuss the question of how information security resources can be managed in effective and economically efficient ways. In the presence of budget constraints, key economic questions for organizations pertain to the level of protection needed by specific assets (processes, systems, etc.), the effectiveness of corresponding countermeasures (e.g., firewalls, intrusion detection systems, security education, or security policies) and the optimal allocation of security budgets (Anderson and Schneier, 2005; Gordon and Loeb, 2006b).

These economic challenges of information security have generated a considerable interest in the academic literature and extant research has addressed different aspects of managing information security investments drawing on micro-economics (e.g., Grossklags et al. (2008)), finance (e.g., Buck et al. (2008)), risk management (e.g., Hoo (2000) or Yeo et al. (2014)) and organization theory (e.g., Cohen (2006)). These approaches address different aspects of information security investments:

I structure the presentation of the large body of research on information security investments along the two areas of decision-making, i.e. planning and evaluation. When it comes to information security investment decision-making, firms are influenced by various factors and aspects: Cultural characteristics and the development of the country affect the company's opportunities and choices in the area of information technology, in particular with regard to information security investments (Khansa and Liginlal, 2009; Melville et al., 2004; Shane, 1994). In addition, firms have to be compliant with country-specific regulations, which require them to spend on precautions to guarantee the confidentiality, integrity and availability of sensitive information because the firm will otherwise have to pay fines and may lose customers (Ghose and Rajan, 2006; Khansa and Liginlal, 2009).

Industry specific regulations, e.g., for the United States include the Sarbanes-Oxley Act (SOX) or the Fair Credit Reporting Act (FCRA) for accounting firms, the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH) for healthcare firms or the Energy Policy Act (EPAct) for firms in the energy sector (Chai et al., 2011; Khansa and Liginlal, 2009; Kiely et al., 2006; Kwon and Johnson, 2014). Information security management standards such as the ISO/IEC 27000 series (Fenz et al., 2011; Glisson and Welland, 2014; Malandrin and Carvalho, 2013; Vuorinen and Tetri, 2012) or the standards of NIST (Bojanc and Jerman-Blažič, 2008, 2012; Chew et al., 2008; Salisbury et al., 2015) are commonly applied in organizations (Siponen, 2006). Moreover, partner firms, Original Equipment Manufacturers (OEMs) and customers influence information security investment decisions, in particular when it comes to information sharing and outsourcing. Much research focusses on the costs and benefits of sharing data on security breaches, threats and potential solutions with so called Information Sharing Alliances (ISAs) (e.g., Anderson and Choobineh (2008); Gal-Or and Ghose (2005); Gordon et al. (2003); Rowe (2007)). Problems related to information sharing are, for instance, reputational risks, sign of weakness to competitors and a decline in financial performance (Gal-Or and Ghose, 2005). Outsourcing has also been investigated in the literature regarding outsourcing of security management to so called Managed Security Service Providers (MSSPs) and regarding outsourcing of non-security-related processes and operations, which is also of security relevance (Alner, 2001; Fink, 1994; Goodman and Ramer, 2007; Hui et al., 2012; Khalfan, 2004), but estimating the real costs of outsourcing is considered a complex problem (Ang and Straub, 1998). In the organization, decisions to invest in information security resources and security processes are made. To support this decision-making with regard to technological and human resources, different approaches have been suggested in the academic literature: VaR approaches (Lee et al., 2011; Wang et al., 2008) and expected utility theory (Huang and Behara, 2013) are applied. For example, VaR approaches have been used in profit optimization models for customer information security investments (Lee et al., 2011) and to examine the risk of daily losses a firm is exposed to because of security incidents (Wang et al., 2008). Expected utility theory was applied to develop an analytic model for information security investment allocation of a fixed budget (Huang and Behara, 2013). Moreover, cost-benefit analysis is used in the literature to determine the optimal selection of countermeasures in information security planning to avoid or mitigate security threats (Sawik, 2013). Financial analyses help to identify the assets, threats, vulnerabilities of information systems and provide an approach for the necessary investment (Bojanc and Jerman-Blažič, 2012) and to evaluate the value of portfolios of various kinds of security countermeasures in the light of different threat and business environments (Kumar et al., 2008). AHP approaches determine the optimal allocation of a budget for maintaining and increasing the security of a firm's information system (Bodin et al., 2005). Game-theoretical approaches are used to identify the amount of information security investments by considering different categories, such as security investments, inherent vulnerabilities, and expected

pay-offs (Cavusoglu et al., 2008) and to interpret and model behavior while negotiating and deciding on security investments (Reniers and Soudan, 2010). Besides the aforementioned approaches to decide on investments in information security resources, (the investments in and implementation of) security processes are an important issue at the firm level. Security processes guarantee an uninterrupted operation of business processes, which is crucial for successful business (Jakoubi et al., 2009) since *"the information security process adds value to the enterprise by reducing the level of risk that is associated with its information and information systems"* (Purser, 2004). Beyond the pure existence of security processes, their quality is decisive: A poor security process provides a false sense of security (Siponen, 2006). The importance of security processes and their connection to business processes has been discussed in the literature (Khansa and Liginlal, 2009; Purser, 2004; Siponen, 2006).

The evaluation of investments in information security resources, such as firewalls, Intrusion Detection Systems (IDS), Chief Information Security Officers (CISO) or workshops, has been covered extensively in the literature. Methods and models for evaluation have been suggested, for instance, by Bistarelli et al. (2012); Bodin et al. (2005); Cavusoglu et al. (2004b); Chou et al. (2006); Bistarelli et al. (2012); Bodin et al. (2005); Cavusoglu et al. (2004c); Chou et al. (2006); Cremonini and Martini (2005); Jing (2009); Locher (2005); Sheen (2010); Wang et al. (2011). Evaluation processes determine whether the invested countermeasures help decreasing risk or whether additional controls are necessary (Barnard and von Solms, 2000; Ekelhart et al., 2009; Knapp et al., 2009; Vroom and von Solms, 2004). Several metrics have been introduced to measure improvements in the overall organizational performance rooted in information security investments, for example, metrics that quantify the Return On Security Investment (ROSI) (e.g., Böhme and Nowey (2008); Gordon and Loeb (2002a)), the Internal Rate of Return (IRR) (e.g., Buck et al. (2008); Wawrzyniak (2006)), Net Present Value (NPV) (e.g., Eisenga et al. (2012); Sheen (2010)), Annual Loss Expectancy (ALE) (e.g., Cremonini and Martini (2005); Tanaka et al. (2005)) or Cumulated Abnormal Return (CAR) (e.g., Andoh-Baidoo and Osei-Bryson (2007); Campbell et al. (2003)).

However, the overall landscape of research contributions is still missing studies regarding relevant aspects of information security investment decision-making and evaluation: The plethora of research articles need to be condensed and their interrelations need to be studied in detail. Moreover, academic models considering the relation between the planning and evaluation of information security investments in combination with the learning of past investment decisions for the future have not been developed yet. In particular, the mutlitude of influences that drive the organizational information security investment decision-making need to be examined and brought to a common denominator. Real-world applicable methods and models to evaluate information security investment decisions, i.e. to measure changes in the organizational performance caused by information security investment decisions are missing so far. Furthermore, learning in the context of information security investments, has not been studied sufficiently yet: As dicussed above, the evaluation of information

security investments has been covered exhaustively; However, it has not been studied yet how the results of the evaluation can be used to adapt and improve future organizational information security investment decisions through learning and which learning strategy should be applied under which circumstances.

In this thesis, I focus on the planning and evaluation of organizational information security investments, i.e. I regard both the models and methods applied for firms' decisions to invest in information security and the evaluation of the investments' efficiency and effectiveness afterwards. Regarding both the planning and evaluation of information security investments is of particular importance for both organizations and academics: Practitioners benefit from this view because this perspective reflects the organizational procedure of planning investments and evaluating them thereafter: Firms plan their information security investments in a structured way to optimize the allocation of their limited information security budget to specific information security countermeasures using decision support models and methods. After having invested, firms evaluate their investment decisions to check whether the implemented information security countermeasures are efficient and effective. For example they check whether the investment in a biometric authentication system was worth the costs because the number of false positiv authentications has decreased. Academics benefit from my perspective considering both organizational planning and evaluation of information security investments because my birds-eye view on information security investments allows to identity gaps in existing research that would otherwise have remained undetected. For instance, the concept of organizational evaluation of information security investments is not sufficiently examined so far and offers a huge area for future research.

1.2 A Theoretical Perspective on Planning and Evaluation of Information Security Investments

In this section, my research is embedded into an overarching and coherent framework of information security investment literature: First, I introduce the research framework which is based on the *Cyber Security Investment Decision Theory* of Rowe and Gallaher (2006). Thereafter, I frame the existing academic literature on information security investments' planning and evaluation with an extension of the *Cyber Security Investment Decision Theory* of Rowe and Gallaher (2006). Based on this framework, the research questions that are adressed in this thesis are derived and the applied research methods are summarized.

1.2.1 The Research Framework

I adapt the *Cyber Security Investment Decision Framework* of Rowe and Gallaher (2006) in order to build a coherent framework to outline existing academic research in the area of planning and evaluation of information security investments. The *Cyber Security Investment Decision Framework* of Rowe and Gallaher (2006) focusses on organizational cyber security decision processes considering factors that influence firms regarding their investments and information resources that firms rely on when it comes to information security investments. For this thesis, I extend the *Cyber Security Investment Decision Framework* of Rowe and Gallaher (2006) to the *Cyber Security Investment Framework for Planning and Evaluation* to cover both planning and evaluation of information security investments.

The Cyber Security Investment Decision Framework

The original model of Rowe and Gallaher (2006) as depicted in Figure 1, aims to investigate the organizational decision-making process related to investments in cyber security in a structured way and therefore covers the planning part of this thesis. The model is described as *"a diagram of the flow of decision-making and the information sources that act as inputs to this process"* (Rowe and Gallaher, 2006). The framework links the constructs *drivers*, *resources*, *investment strategy*, *implementation strategy*, *budget allocation process*, *cyber security infrastructure* and *nature and frequency of cyber security breaches* in a "has impact on"-way.

In the center of the model is the cyber security investment decision process which is influenced by certain factors and impacts the cyber security infrastructure. As depicted in Figure 1, the *Cyber Security Investment Decision Process* consists of two phases: the *Investment Strategy* and the *Implementation Strategy* which are described thereafter: The *Investment Strategy* refers to the management's determination of security investment priorities considering overall business operations, cost minimization and the information security budget (Rowe and Gallaher, 2006). The investment strategy is influenced by internal and external *Drivers* (Rowe and Gallaher, 2006; Daneva, 2006; Su,

2006). External drivers include regulations or demands of suppliers or clients (Rowe and Gallaher, 2006; Cavusoglu et al., 2015; Johnston and Hale, 2009). Internal drivers are, for instance, the need to protect business processes or past security breaches (Tanaka et al., 2005; Tatsumi and Goto, 2010; Hausken, 2006). The main drivers are legality requirements, e.g. the Sarbanes Oxley Act, which demands compliance and puts pressure on the organizations (Cavusoglu et al., 2015; Johnston and Hale, 2009). Those drivers affect organizations' investments strategy because they force firms to invest in certain information security measures (Johnston and Hale, 2009; Laudon and Laudon, 2015).

The *Implementation Strategy* refers to the IT staff's determination of the most efficient approach to meet the security needs with evaluating and comparing specific security solutions and deciding whether to use a reactive or proactive security strategy (Rowe and Gallaher, 2006). The implementation strategy is influenced by internal and external *Resources*: Resources refer to software, hardware, policies, processes and procedures which are already implemented within the organization (internal) or available to purchase and implement in the future (external) (Rowe and Gallaher, 2006; Barnard and von Solms, 2000). Internal resources which are already implemented in the firm influence the implementation strategy because the organization need to ensure that the newly acquired resources fit into the existing system (Barnard and von Solms, 2000). Moreover, external resources influence the firm's implementation strategy as organizations consider every available security control on the market (Barnard and von Solms, 2000).

The *Budget Allocation Process* is separate from the decision process and influences the implementation strategy: After having determined the adequate amount to invest, the firm should allocate this limited information security budget to certain information security solutions in order to prevent security incidents (Rowe and Gallaher, 2006; Gordon and Loeb, 2002b). Therefore there is an interrelation between the budget allocation process and the implementation strategy. The arrow from the implementation strategy to the budget allocation decribes the feedback between a firm's strategy for security and the budget it sets for information security: The implementation strategy influences the budget allocation because - dependent on the resources and the investment strategy - there may be more or less information security budget necessary to carry out the planned implementation strategy, i.e. the given information security budget may be altered and adapted to the needs identified in the implementation strategy. Accordingly, this interrelation between the implementation strategy and the budget allocation process decribes the trade-off between the level of security and the budget: A firm that aims to optimize their information security level might spend a lot of money whereas an organization seeking to comply with a given limited information security budget might not reach an adequate level of security.

As the investment strategy refers to the management's determination of security investment priorities considering the information security budget (Rowe and Gallaher, 2006), there is also an interrelation between the investment strategy and the budget allocation process: The overall

information security budget determines the allocation of this budget. Consider, for instance a firm which has set a very restricted information security budget and therefore no money can be allocated to information security workshops to train employees.

The cyber security investment decision process has an impact on the *Cyber Security Infrastructure* of the organization as the adoption of new technologies, policies, or procedures improves security and increases the security level with meeting internal security objectives or with satisfying government regulations (Rowe and Gallaher, 2006). Usually this impact is positive: Consider for instance a firm which has decided to invest in a firewall. Then the firm's cyber security infrastructure is improved because incoming and outgoing network traffic is monitored and controlled by the firewall. The impact of the cyber security investment decision process on the cyber security infrastructure can be negative for instance when an organization decides to invest in a firewall and implement it where already one firewall is installed because two firewalls may collide.

The firms' cyber security infrastructure determines the *Nature and Frequency of Cyber Security Breaches* (Rowe and Gallaher, 2006): The more efficient an organizational cyber security infrastructure, i.e. the higher the level of security, the less the probability and impact of a successfull information security breach (Sumner, 2009; Gordon and Loeb, 2002b).

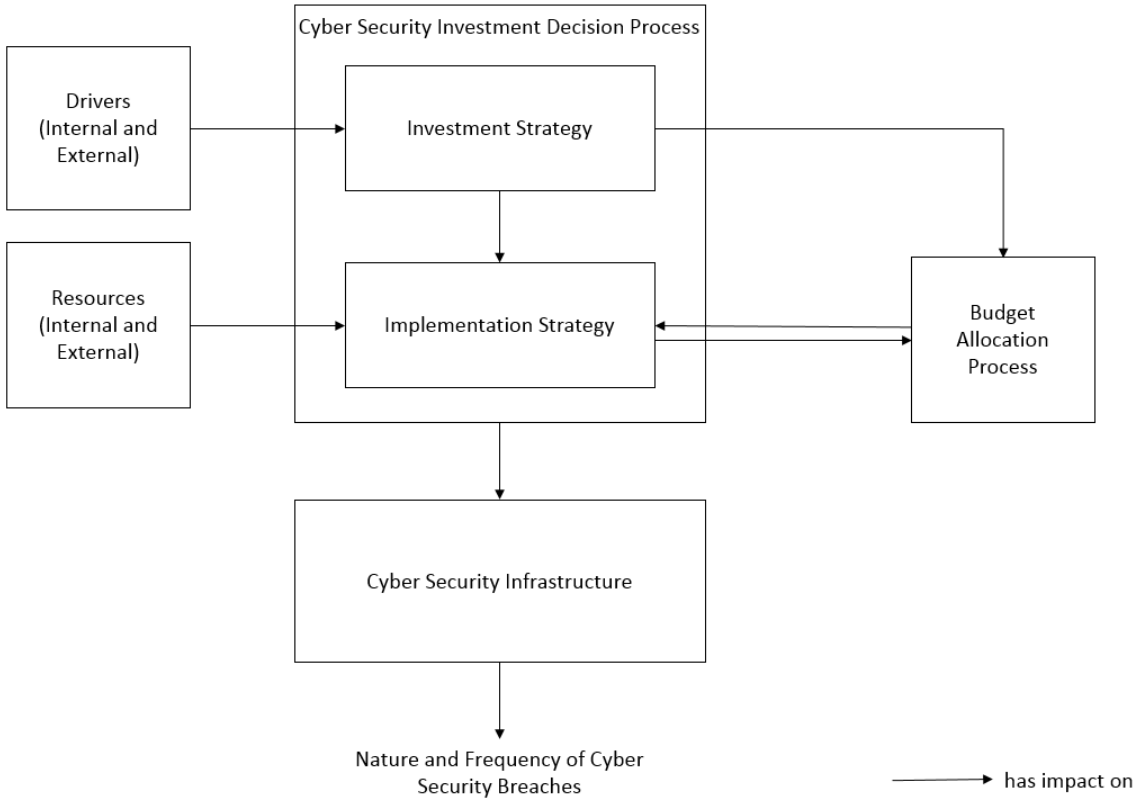

Fig. 1: Cyber Security Investment Decision Framework from Rowe and Gallaher (2006)

The Cyber Security Investment Framework for Planning and Evaluation

The Cyber Security Investment Decision Framework of Rowe and Gallaher (2006) focuses on the organizational information security investment decision making and its results in terms of an improved and adapted cyber security infrastructure and lower probability of cyber security breaches (nature and frequency of cyber security breaches). However, the model does not cover the evaluation of those information security investment decisions. In order to improve future investment decisions, organizations need to evaluate whether their investments have proved to be the right decision (Cavusoglu et al., 2004b; Böhme and Nowey, 2008; Su, 2006): To evaluate the efficiency and effectiveness of their investment decisions, the organizational performance can be used: The organizational performance describes the overall firm performance (Melville et al., 2004) including productivity, efficiency, profitability, market value and competitive advantage (Grant, 1991; Melville et al., 2004; Peteraf, 1993). With the organizational performance firms can justify future investment decisions (Böhme and Nowey, 2008). Therefore, I extend the framework of Rowe and Gallaher (2006) to cover not only the decision-making but also the organizational evaluation of information security investments in order to create a model for this thesis.

To include the evaluation of information security investments I extend the Cyber Security Investment Decision Framework from Rowe and Gallaher (2006) in the following way. I added the construct *Organizational Performance* and an arrow from the cyber security investment decision process to the organizational performance into the framework for the following reason: The cyber security investment decision process from the original model leads to organizational information security investments in hardware, software, processes or policies which results in changes of the organizational performance in terms of market value or security level (Rees et al., 2003). Therefore the organizational performance indicates the effectiveness and efficiency of the undertaken information security investments (Su, 2006; Drugescu and Etges, 2006; Pfleeger and Rue, 2008; Finne, 1998). Note that the organizational performance can be influenced by information security investments not only in a positive way: If the new authentication system is more restrictive than the old one, many employees will be mistakenly blocked when trying to get access to the premises of the firm. As a consequence, workflows become interrupted, which can result in interrupted business operations and a decline in organizational performance.

Moreover, I added an arrow from the organizational performance to the cyber security investment decision process for the following reason: For future information security investment decisions, organizations can use the results of the evaluation and learn from them to make adequate decisions in the future, i.e. the organizational performance of the past can result in adapted information security investment decisions through learning. As attackers learn from their past errors and find new ways to exploit vulnerabilities, firms need to adapt to their circumstances as well (Gupta et al., 2011). Learning from past actions and security decisions permits an organization to switch to more cost-effective technologies and achieve better future protection from attackers at lower cost (Khansa

and Liginlal, 2009; Franqueira et al., 2010). An example for learning in practice is the following: Consider a firm whose investments in workshops effect a decline of unintended security incidents, then the organization will learn from the effectiveness and will intensify future investments in such trainings. Another example is the investment in a different anti-virus program when the detection of malware has turned out to be unacceptably bad. This relationship is illustrated with the arrow from the organizational performance to the cyber security investment decision process.

Moreover, I added a link from the nature and frequency of cyber security breaches to the organizational performance because severe and iterated security breaches influence the firm's organizational performance in a negative way regarding their reputation, market value, profitability and competitive advantage (Hovav et al., 2007; Goel and Shawky, 2009; Campbell et al., 2003). In terms of market value, information security breaches result in significant negative stock market return for the breached organization (Hovav et al., 2007; Goel and Shawky, 2009; Campbell et al., 2003).

In Figure 2 the extention of the Cyber Security Investment Decision Framework of Rowe and Gallaher (2006), namely the *Cyber Security Investment Framework for Planning and Evaluation* is depicted.

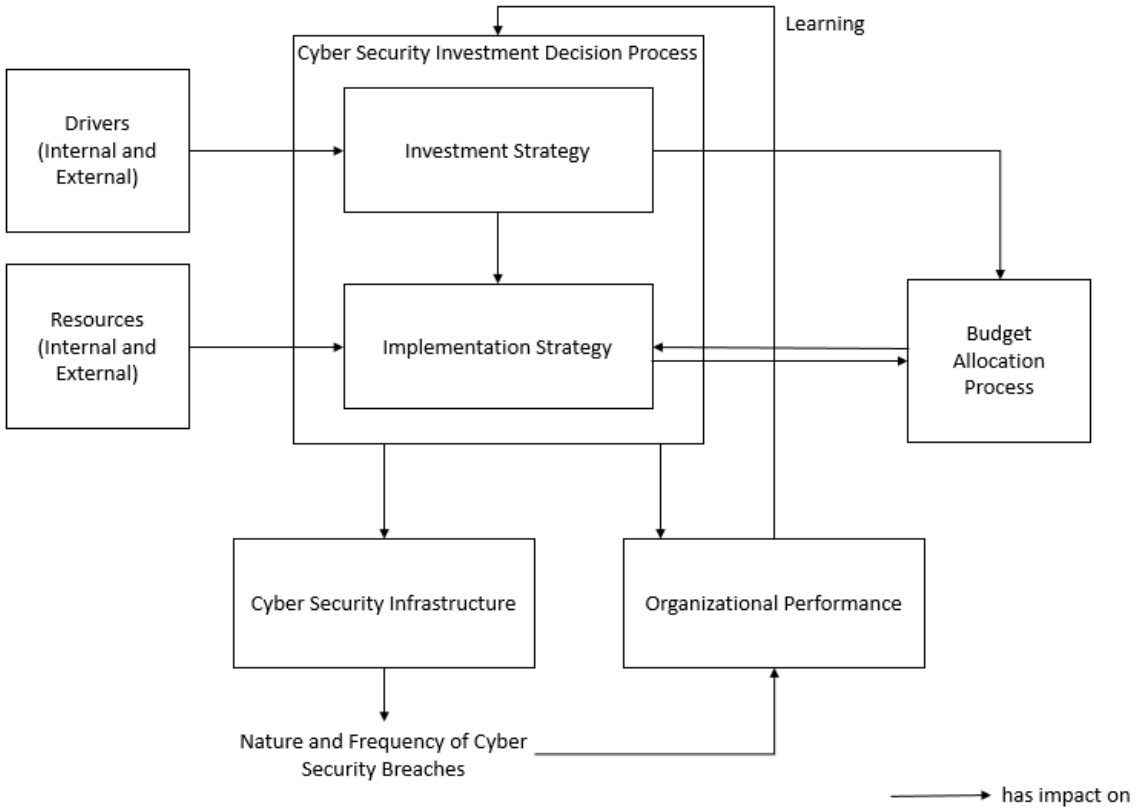

Fig. 2: Cyber Security Investment Framework for Planning and Evaluation based on Rowe and Gallaher (2006)

1.2.2 Research on Information Security Investments

In the following I provide an overview of academic literature on information security investments for planning and evaluation framed by the introduced Cyber Security Investment Framework based on Rowe and Gallaher (2006).

Research on Planning of Information Security Investments

"Planning information security investment is somewhere between art and science" (Böhme, 2010, p. 1) and has been a research subject since the turn of the millennium when the articles of Anderson in 2001 and Gordon and Loeb in 2002 drew attention to the topic of information security investment planning (Anderson, 2001; Gordon and Loeb, 2002b; Schatz and Bashroush, 2017).

Drivers

Organizations' decisions to invest in specific information security countermeasures are influenced by external and internal drivers which have been examined in academic literature. Four important drivers have been identified (Daneva, 2006; Su, 2006): Government and industry-sector specific regulations, standards, such as ISO 17000, and best practice models like ITIL and COBIT and risks and business requirements of the specific industry. The main drivers are legality and compliance requirements (Cavusoglu et al., 2015; Johnson, 2009). In the context of information security, examples for such regulations include Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security ManagementAct (FISMA), the Sarbanes Oxley (SOX) Act, California SB 1386 or the European Unions Data Protection Directives (Cavusoglu et al., 2015). These regulations demand compliance and therefore put pressure on the organizations. For example, the Payment Card Industry Data Security Standards (PCI DSS) regulates the sensitivity of credit card data, dictates access control requirements and encryption techniques for transmission and storage of specific data. Accordingly, this regulation forces the involved firms to invest in corresponding information security measures. Considering that compliance with these regulations require information security investments so that organizations can stay in business (Johnson, 2009; Laudon and Laudon, 2015), compliance is the most important information security investment driver.

Besides these external drivers, academic literature names internal drivers such as vulnerability (Tanaka et al., 2005; Hausken, 2006), threats (Tatsumi and Goto, 2010), uncertainty, potential loss (Huang et al., 2014) and risk (Finne, 1998; Bodin et al., 2008; Wang et al., 2008) as information security investment drivers (Johnson, 2009). The influences of these drivers on firms' investment strategy has been examined in detail. Reseach indicates that organizational information security investment decisions depend on vulnerability: If the vulnerability levels are low or extremely high, then firms do not make higher than usual expenditures in information security (Tanaka et al., 2005;

Liu et al., 2008). However, firms invested more than usual if the vulnerability levels are medium-high (Tanaka et al., 2005; Liu et al., 2008). Moreover, it was shown that, higher threat levels cause both larger and later organizational investment expenditures, while lower threat levels lead to immediate but lower investments (Tatsumi and Goto, 2010). Concentrating on information security investements in the healthcare sector, Huang et al. (2014) examined information security investments based on various threat environments and found out that fear of potential losses drive firms to invest in information security, but investment is only triggered when the potential loss reaches a threshold level (Huang et al., 2014). In addition, it has been studied how the business benefits from information security investments and how these benefits act as a driver to influence firms' investment decisions (Huang et al., 2014). Regarding the level of risk as driver, extreme value analysis has been used to quantify the risks of information security and to determine proper security solutions based on a firm's risk preference (Wang et al., 2008). An extensive list of information security investment drivers can be found in Johnson (2009).

Resources

When it comes to information security investments, internal and external resources influence the organizational implementation strategy. Internal resources, such as hardware and software which are already implemented in the firm need to be considered in the information security investment decision making process because newly acquired resources need to fit into the existing system (Barnard and von Solms, 2000). The interaction between different security resources is important, since a defense-in-depth security architecture is advised, i.e. it is recommended to implement more than one safeguard against threats (Su, 2006). Accordingly, it is important to study whether resources complement each other, for example, is a system with both a firewall and an intrusion detection system more efficient than when each control is applied individually (Su, 2006)?

External resources influence the decision making because firms try to implement every available security solution that the market has to offer (Barnard and von Solms, 2000). In addition, external resources might be less expensive or more efficient than internal resources which might lead to the decision to replace existing resources with new ones. Information security resources have been studied extensively in academic literature: Such resources are often classified into three sequential categories, namely prevention (e.g., firewall), detection (e.g., intrusion detection system) and recovery (e.g., monitoring systems) (Straub and Welke, 1998). Those three categories indicate for what specific purpose a security solution is implemented: Prevention methods stop a threat from succeeding and detection and recovery mechanisms reduce the attack's damage when the attack has been sucessful (Su, 2006). Additionaly, academics distinguish between technical and human information security resources (Gordon and Loeb, 2002b). Technical defenses include encryption techniques, firewalls or access controls while human resources focus on behavioural aspects of information security: Human information security resources include, for instance, awareness trainings for employees (Gordon and

Loeb, 2002b). Determining the effectiveness of such resources is difficult and controversial (Su, 2006). Studies concentrating on the implementation of information security resources are manifold: For example, a mathematical model for dynamically and economically investing in cloud firewalls with respect to actual needs is developed (Yu et al., 2013). When it comes to investing in human resources, research highlights the importance of rising security awareness among both managers and employees (Straub and Welke, 1998; Whitman, 2003). However, studies showed that firms do not invest enough to raise awareness (Kruger and Kearney, 2006).

Cyber Security Investment Decision Process

Before investing in information security solutions, decision makers want to make sure that the investment is financially justified (Sonnenreich et al., 2006). Therefore, methods, models and metrics are used to show how possible information security investments might impact and benefit the organization's business because for organizations it is important that security makes *"business sense"* (Su, 2006), for example offer new services or attract new customers. An organization's management tries to balance between risks and the costs of security solutions to reduce these risks: *"Perfect security does not exist, and even if it exists, it may very well be too expensive and not worth it."* (Su, 2006). Literature points out that the first rule of information security is *"that you should never spend more to protect something than that thing is actually worth"* (Crume, 2000). Accordingly, the costs for a security solution must not exceed the value of the assets that the security solutions tries to protect (Su, 2006). Therefore, organizations need to determine the value of their assets and the true costs of information security breaches in order to efficiently manage their information security investments (Spencer, 2000). Various valuation methods have been introduced to measure the explicit costs (e.g., costs of reinstalling and reconfiguring software) and the implicit losses (e.g., losses in future sales because of damaged reputation and decreased customers' trust) of information security breaches (Cavusoglu et al., 2004c; Campbell et al., 2003; Su, 2006).

Information security investment and implementation strategies have been extensively studied in academic literature. Using input from internal and external drivers, the investment strategy influences the firm's budget allocation (Rowe and Gallaher, 2006). The investment strategy indicates the firms' information security investment priorities (Rowe and Gallaher, 2006). For example, some firms' management views the minimization of probability of successful security breach as their top priority and therefore invest in various security controls. Others may regard the smooth and continuous running of the business process as most important (Johnson, 2009). Since implementing new security controls often requires stopping business processes, this investment strategy may not lead to new and potentially necessary information security investments. Note that information security investment priorities depend on the position of the decision-makers within the firm: While security experts prioritize risk minimization, managers focus on business continuity (Johnson, 2009).

However, information security investment decision-making is task of the management and therefore business continuity is uppermost on the list of priorities (Johnson, 2009).

The organization's implementation strategy refers to determining the most efficient information security investments (Rowe and Gallaher, 2006). The implementation strategy is influenced by the investments strategy considering the firm's level of security and the budget for information security (Rowe and Gallaher, 2006). There is a trade-off between the level of security and the information security budget: A firm that aims to optimize their information security level might spend a lot of money whereas an organization seeking to comply with a given limited information security budget might not reach an adequate level of security. The level of security that an organization aims to accomplish is determined by identifying security needs and priorities (Rowe and Gallaher, 2006). Accordingly, firms identify existing security vulnerabilities within the organization and the most valuable assets they seek to protect. Moreover existing threats both internal and external are identified in order to implement security countermeasures accordingly (Belanger et al., 2002; Bistarelli et al., 2006; Breier and Hudec, 2013; Ljungdahl and Nordström, 2016). Information security countermeasures comprise technical countermeasures including firewalls, antivirus software or encryption techniques, operational countermeasures including physical access controls and backup capabilities and management countermeasures including policies and employee training (Baker and Wallace, 2007; Stoneburner et al., 2002). The implemented security countermeasures protect the assets from harm through threats (Weishäupl, 2017). Thus implementing a security countermeasure aims to close, or at least reduce, a vulnerability. Assets are affected by vulnerabilities and threads exploit these vulnerabilities, if they are not protected by a corresponding security countermeasure. For example, the asset data can be affected by the vulnerability lack of training and the threat employee can exploit this vulnerability. The associated countermeasure is a security workshop to train employees (Weishäupl, 2017). With this strategy a firm's security needs and priorities can be identified. Accordingly, the investment strategy influences the implementation strategy because organization which focus on optimizing their level of security have another implementation strategy than firms concentrating on meeting a limited information security budget (Rowe and Gallaher, 2006).

The implementation strategy is affected by the resources which are already implemented in the organization or which are available on the market and by the budget (Rowe and Gallaher, 2006). Academic literature provides a plethora of approaches in this area: Traditional cost benefit analysis has been used which requires identification of the assets and the financial consequences and risks of security incidents and the costs of security controls (Dutta and McCrohan, 2002). Moreover, the game tree approach (Grossklags et al., 2008; Cavusoglu et al., 2008; Wu et al., 2015), the rating method of the analytic hierarchy process (Bodin et al., 2005; Cheng and Li, 2001) and decision analysis (Hoo, 2000) are applied. In addition to these decision theory based approaches, economic methods are applied, namely game theory and traditional risk-return analysis (Cavusoglu et al., 2004a; Huang et al., 2008). Game theory allows to examine the behaviour of attackers and model

the interaction between an organization and attackers (Huang et al., 2008). Since firms face strategic adversaries, i.e. attackers who are exploiting the firms' vulnerabilities, researchers view information security as a game between organizations and attackers (Su, 2006). Research indicated, for instance, that investing in such an intrusion detection system leads to a positive return only when the detection rate is higher than a threshold which is obtained by the cost and benefit parameters of the attackers (Cavusoglu et al., 2005). Note that academics advises not to use traditional financial analysis in the area of information security investment because it is ineffective (Wood and Parker, 2004).

The Budget Allocation Process

Since no firm can be completely secure without unlimited budget, it is important for an organization to know what the "right amount" of investment is (Huang et al., 2014). Intuition might suggest that the optimal amount to invest in information security is an increasing function of the information's vulnerability (Gordon and Loeb, 2002b). However, research indicates that the optimal information security investment amount is first increasing and then decreasing as vulnerability increases (Gordon and Loeb, 2002b). To determine the optimal level of information security investments, various approaches have been applied: Gordon and Loeb provide an economic framework for assessing the optimal amount to invest in information security to protect a given set of assets (Gordon and Loeb, 2002b). It has been shown that there exists an upper limit for the level of optimal security investments in relation to the total cost of the protected information assets (Willemson, 2006; Gordon and Loeb, 2002b). However, in practice, the information security budget is heavily dependent on the past years budget or best practices (Gordon and Loeb, 2006a). The model of Gordon and Loeb has been extended by a timing dimension, by productivity spaces, modified and improved by Bodin et al. (2005), Gordon et al. (2015), Willemson (2006), Matsuura (2009), Wang et al. (2011) and Tatsumi and Goto (2010).

There is an interrelation between the budget allocation process and the implementation strategy represented by two arrows in Figure 2 which will be discussed in the following: After having determined the adequate amount to invest, the firm should allocate this limited information security budget to certain information security solutions in order to prevent security incidents. Academic literature provides hereto approaches and models: Considering two types of security attacks, namely targeted and opportunistic, research found out that organizations should allocate the most part of their limited information security budget to defend against targeted attacks (Huang and Behara, 2013; Huang et al., 2006). Regarding the feedback from the implementation strategy to the budget allocation, I observe that this feedback often takes place in practice as noticed by Rowe and Gallaher (2006) but has not been adequately studied by academics: The implementation strategy may influence the budget allocation because - dependent on the resources and the investment strategy - there may be more or less information security budget necessary to carry out the planned implementation strategy, i.e. the given information security budget may be altered and adapted to the

needs identified in the implementation strategy. Note that, over-investing in information security controls is common in organizations: Managers try to reduce the probability of security incidents during their tenure in order to boost their reputation (Srinidhi et al., 2015).

Research on Evaluation of Information Security Investments

Firms reflect on decisions made in the past and evaluate whether their strategy was effective and efficient (Böhme and Nowey, 2008), i.e. they learn from past experiences: Organizations learn when they *"draw lessons from past successes and failures, and detect and correct errors of the past, anticipate and respond to impending threats, engage in continuous innovation, and build and realize images of a desirable future"* (Quaye and Harper, 2014, p. 10).

Cyber Security Infrastructure

A cyber security infrastructure for effective security, privacy and data protection is influenced by information security investments, i.e. by the cyber security investment decision process: If the firm decides to invest in another information security countermeasure to raise its level of security, the cyber security infrastructure is improved in terms of increased level of security, privacy or data protection (Hooper, 2009).

The cyber security infrastructure determines the nature and frequency of information security breaches: The more efficient an organizational cyber security infrastructure, i.e. the higher the level of security, the less the probability and impact of a successfull information security breach (Sumner, 2009; Gordon and Loeb, 2002b).

Nature and Frequency of Cyber Security Breaches

The nature of cyber security breaches can be assessed through five characteristics (Hovav et al., 2007): The attackers' intention (e.g., vandal, hacker, professional criminal or terrorist), their objectives (e.g., damage, challenge or financial gain), the results they achieve (e.g., corruption of information, disclosure of information or denial of service), the tools used (e.g., scripts, programs or autonomous agents) and the access (unauthorized use or access) (Hovav et al., 2007).

The nature and frequency of cyber security breaches have an influence on the organizational performance. Organizations that are repeatedly und successfully attacked will experience a decrease in their organizational performance. Academic reseach found out that information security breaches effect abnormal stock market return depending on the breach characteristics (Hovav et al., 2007; Goel and Shawky, 2009; Campbell et al., 2003). The type of attacker and his objective have a significant impact on the market reaction: Attacks by professional criminals and attacks intended for financial gain resulted in significant negative market reaction (Hovav et al., 2007). However, the most significant characteristic is the result of the attack: Breaches resulting in disclosure of private

information had a significantly larger effect on the stock market return while denial of service attacks and corruption of information had less impact (Hovav et al., 2007).

The Organizational Performance

Information security investments result in increased organizational performance, e.g., in terms of stock market return: Organizations that publicly announce information security investments are rewarded with a higher cumulated abnormal stock market return (Chai et al., 2011; Brock and Levy, 2013; Bose and Leung, 2013; Xu et al., 2017). The stock market's reaction to various types of information security investments has been regarded in academic literature, e.g., investments in identity theft countermeasures or investments with commercial exploitation (Chai et al., 2011; Brock and Levy, 2013; Bose and Leung, 2013; Xu et al., 2017).

Traditional financial metrics such as return on investment (ROI), net present value (NPV), and the internal rate of return (IRR) have been developed to measure the organizational performance (Drugescu and Etges, 2006; Pfleeger and Rue, 2008). The most commonly used metric in practice is the ROI, followed by the IRR (Su, 2006). However, such metrics can not quantify the intangible benefits of information security (Finne, 1998). Therefore other approaches have been applied: Based on the assumption that organizational information security investments affect the market value of the investing firm, studies investigate the stock market reaction to information security investments of publicly traded firms. With this methods, intangible benefits of investments, like the firm's reputation, customers' trust or competitive advantages can be measured (Chai et al., 2011). It was shown that information security investments with commercial exploitation lead to higher abnormal stock market return than information security investment for information security improvement (Chai et al., 2011). Regarding the impact of organizational performance on future decision-making, i.e. learning, research provides the following results: Proactive information security investments for commercial exploitation lead to higher return, i.e. higher organizational performance than investments for information security improvement (Xu et al., 2017). For reactive information security investments the opposite is the case (Xu et al., 2017). This study provides guidance for managers on how to make effective and efficient information security investment decisions in the future: It is recommended that managers should consider this correlation between their investment strategy and the investment timing because otherwise they may obtain negative stock market return (Xu et al., 2017). Furthermore, organizations benefit from proactive information security investments in order to achieve competitive advantages (Xu et al., 2017). However, for improving their information security reactive investments are advised (Xu et al., 2017). When it comes to investing in identity theft countermeasures, research indicate that the market rewards early adopters and adopters of sophisticated measures (Bose and Leung, 2013). Therefore, the authors suggest to implement identity theft countermeasures at an early time (Bose and Leung, 2013).

1.2.3 Research Questions

In the following the research questions which are subject of the investigation in this thesis are derived from the Cyber Security Investment Framework for Planning and Evaluation (Rowe and Gallaher, 2006).

In essence, research has produced a substantial body of knowledge on information security investments (c.f. Section 1.2.2). That research aims at examining drivers and resources, including software, tools, systems and personnel. As depicted in the Cyber Security Investment Framework for Planning and Evaluation, the drivers and resources influence the cyber security investment decision process because they force organizations to invest in certain security controls. This influence of drivers and resources on the cyber security investment decision process has been examined in various research articles, e.g., Daneva (2006); Su (2006); Cavusoglu et al. (2015); Johnston and Hale (2009); Barnard and von Solms (2000); Wang et al. (2008); Straub and Welke (1998). To structure the plethora of research articles, researchers have provided several literature reviews (e.g., Fernández-Alemán et al. (2013); D'arcy and Herath (2011); Karlsson et al. (2016); Lebek et al. (2013); Silic et al. (2015); Soomro et al. (2016)) with different foci: For example, Fernández-Alemán et al. (2013) report the results of a systematic literature review regarding security and privacy issues in electronic health record systems; Goyal et al. (2010) reviewed the literature on fundamental security attacks in mobile ad hoc networks or Lebek et al. (2013) analyzed information security awareness and behavior of employees by a theory-based literature review. A high diversity in terms of disciplines, methodologies and theories is applied, which account for the multi-faceted nature of organizational information security investments. However, a comprehensive literature review of information security investment planning in an organizational context considering drivers and resources, as depicted in Figure 2, in order to identify what we already know is still missing. Therefore, I pose the following research question (RQ):

> RQ1: What insights are provided by existing academic literature on how organizations make decisions on their information security investments under consideration of external and internal drivers and information security resources?

Research question 1 adresses the drivers and resources as well as the link between these constructs and the cyber security investment decision process as illustrated in Figure 3.

Furthermore, I address the practical implementation of the existing academic models and methods on information security investments in real-world organizations. I strive to understand how information security investment decisions are evaluated in firms and how these decisions evolve, i.e. how organizations learn from past investment decisions to adapt future investments which is illustrated by the arrow from the organizational performance to the cyber security investment decision process in Figure 2. As depicted in the Cyber Security Investment Framework for Planning and

Evaluation, the organizational performance influences the cyber security investment decision process through learning: Firms learn from the results of evaluating their information security investment decisions with measuring the organizational performance of undertaken decisions and improve future investment decisions. Several academic articles have already been carried out to investigate organizational behaviour in the context of information security investments for instance to support security investment decision-making (Beresnevichiene et al., 2010) or to investigate the question in which security solutions it is worth investing (Fenz et al., 2011). However, an integrated view focussing on evaluation and organizational learning in the context of information security investments has not been addressed with existing research. Accordingly, I aim to answer the following research question:

> RQ2: How do organizations evaluate their information security investment decisions and how do they learn from past decisions to make more efficient decisions in the future?

Research question 2 adresses the organizational performance and the link between the organizational performance and the cyber security investment decision process as illustrated in Figure 3.

With the third research question, I strive to measure the changes in organizational performance caused by a firm's information security investments which is illustrated by the link from the cyber security investment decision process to the organizational performance in Figure 2: As depicted in the Cyber Security Investment Framework for Planning and Evaluation, the cyber security investment decision process influences the organizational performance because security investments raise the firm's security level and increase the overall firm performance. Metrics and measures to measure the organizational performance and to assess the cost and benefits of information security investments are manifold in academic research as presented above (Drugescu and Etges, 2006; Pfleeger and Rue, 2008; Finne, 1998; Chai et al., 2011; Bose and Leung, 2013; Xu et al., 2017). However, I found out that due to limited data, assessing the costs of information security breaches is a challenging task for firms, i.e. firms do not use the metrics and methods developed in academic literature (Weishäupl et al., 2018). To overcome this problem of limited data, I measure the benefits of information security investments based on an organization's value in the stock market as done in Chai et al. (2011). Hereby, the following research question is addressed:

> RQ3: How do information security investments influence the firm's organizational performance in terms of the stock market value?

Research question 3 adresses the link between the cyber security investment decision process and the organizational performance as illustrated in Figure 3.

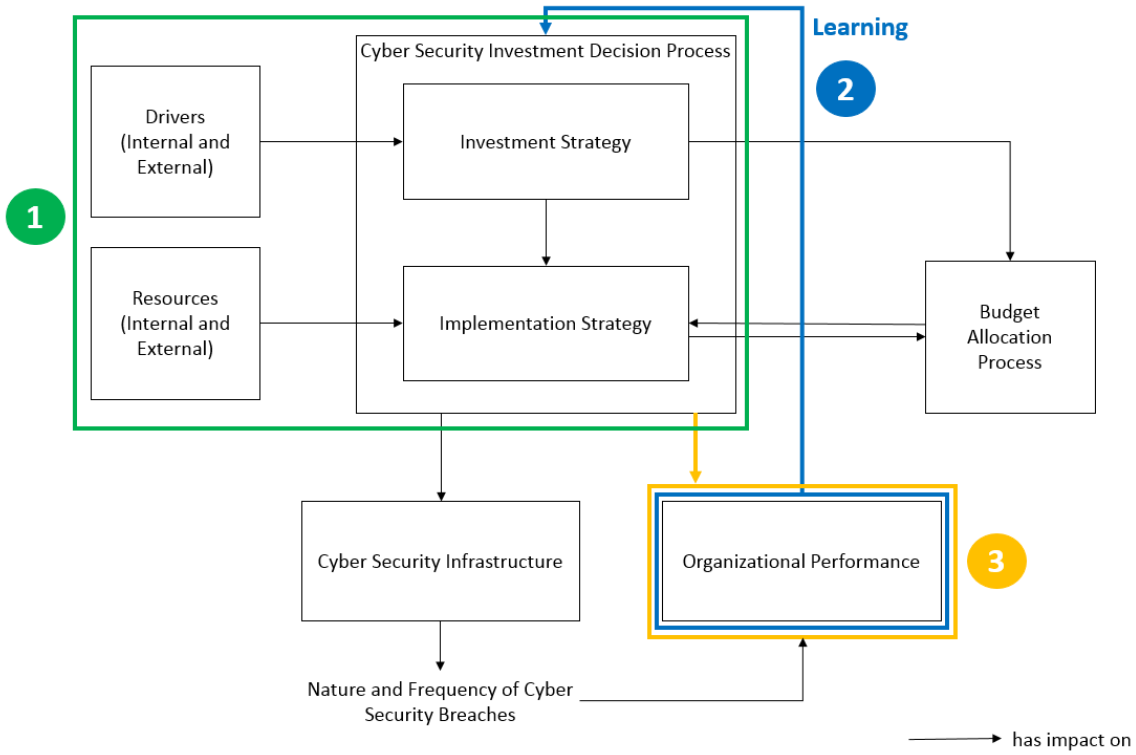

Fig. 3: Presentation of the Research Questions RQ1, RQ2 and RQ3 in the Cyber Security Investment Framework for Planning and Evaluation based on Rowe and Gallaher (2006)

1.2.4 Research Methods

In the following, the applied research methods to answer the introduced research questions are described:

For research question 1 I conduct a comprehensive theory-based review of the literature on organizational information security investments. The underlying theory is a unifying theory drawn on the resource-based view (RBV) and the organizational learning theory (OLT). Relevant literature is identified following four phases: Phase 1 includes a keyword search in pertinent journal and conference databases, in phase 2 the references of those articles will be examined that will have been identified during phase 1. Phase 3 contains the scanning of the abstracts of these research papers and excluding those papers that did not seem to be related to the investigation. Finally, phase 4 analyses the body of these papers regarding their research questions, methodology and research models, and characteristics. After the identification of relevant articles, they are synthesized according to the theory in order to get an overview of the literature and to be able to identify research gaps and guide avenues for further research. This in-depth literature review is an adequate and common methodology to treat research question 1.

To adress research question 2, an exploratory case study is carried out to substantiate the theoretical approach presented in the literature review with insights gained through interviews with

experienced practitioners. I draw on the RBV and the OLT and use this multi-theoretical perspective to conduct an exploratory multiple case study. To understand how information security investment decisions are made and evaluated in organizations and how they learn from past investment decisions, I interview seven consulting organizations and five non-consulting firms whereby the asked questions are derived from the RBV and OLT. I benefit from the integration of the consultants and the non-consultants' answers in three ways: (1) I can combine the first-hand information of the non-consulting firms and the second-hand information gained from the interviews with consulting firms; (2) I can integrate the broad knowledge of the interviewed consulting organizations on the information security management of their many clients and the concentrated knowledge of the interviewed non-consulting firms on their information security management; (3) With not only interviewing non-consulting firms but also consulting firms, I can overcome the deficiency that firms might not want to disclose security-related inadequacies and mistakes to me for fear of attacks and harm of reputation.

In order to answer research question 3, I apply the event study methodology to measure the return on information security investments since stock market return can be used to measure organizational performance (Campbell et al., 2003; Bose and Leung, 2013; Bose and Luo, 2014). Since the event study methodology focusses on studying the effects of public event announcements on stock prices because immediate market response represents the expectations of investors towards a firm's future performance based on the current corporate actions, this methodology is a suitable research method to adress research question 3. Covering the time period from 2000 to 2017, I collected information security investment announcements by electronically searching the Lexis/Nexis Academic Database. The final sample consists of 63 newspaper articles about organizational information security investment announcements. The historical data from the stock market was obtained using Alpha Vantage. For the statistical calculations I apply a two-sample t-test, which is one of the most commonly used hypothesis tests.

Table 1 gives an overview of the relationships between the research questions, the publications and the used research methods.

1.2.5 Contributions

In this subsection the contributions for each paper in this thesis are described in a summarized form.

The academic literature provides many articles on information security investments. However, this material needs a theoretical basis and synthesis which is provided in paper 1. The contributions of this publication to the literature on information security investments are the following: (1) I develop a new theoretical model on information security investments by drawing on two established IS theories, the RBV and the OLT. The two theories are appropriate because they complement each other: the RBV operationalizes and covers major aspects that need to be considered in investment decisions namely at the national, industry or firm level; the OLT takes into account that information technology is dynamically changing which leads firms to adapt their security strategies

Table 1: An Overview of the Publications, the adressed Research Questions and the Research Methods.

Research Questions		**Paper**		**Research Methods**
RQ 1	What insights are provided by existing academic literature on how organizations make decisions on their information security investments under consideration of external and internal drivers and information security resources?	Paper 1	A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory Status: Published in *Proceedings of ICIS 2015*	I conduct a comprehensive theory-based **literature review** on organizational information security investments. The underlying theory is a combination of the RBV and the OLT.
RQ 2	How do organizations evaluate their information security investment decisions and how do they learn from past decisions to make more efficient decisions in the future?	Paper 2	Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning Status: Published in *Computers & Security*	I conduct an exploratory **case study** drawing on the RBV and the OLT. Seven consulting organizations and five non-consulting firms are interviewed.
RQ 3	How do information security investments influence the firms organizational performance in terms of the stock market value?	Paper 3	Timing in Information Security: An Event Study on the Impact of Information Security Investment Announcements Status: Under review at *Decision Support Systems*	I conduct an **event study** to measure the return on information security investments. For the statistical calculations I apply a two-sample t-test.

and investments accordingly. (2) Based on this new multi-theoretical perspective, I synthesize the existing information security investment literature. The new model additionally allows to identify research gaps and to derive research questions which would otherwise have remained unidentified in order to stimulate future research on this topic. The discussed managerial implications highlight that answering the identified research questions and addressing the related gaps have not only academic relevance: I provide examples of how managers would benefit from answering the research questions. All in all, as paper 1 focuses on the academic literature on information security investments, research question 1 is answered.

Paper 2 contributes to the literature on information security investment by providing an unadulterated overview over organizations' investment decisions, evaluations and learning strategies. I benefit from the integration of the consultants' and the clients answers in three ways: (1) I can combine the first-hand information of the non-consulting firms and the second-hand information

gained from the interviews with consulting firms; (2) I can integrate the broad knowledge of the interviewed consulting organizations on the information security management of their many clients and the concentrated knowledge of the interviewed non-consulting firms on their information security management; (3) With not only interviewing non-consulting firms but also consulting firms, I can overcome the deficiency that firms might not want to disclose security-related inadequacies and mistakes to me for fear of attacks and harm of reputation. Hence, with combining these two perspectives, I provide (1) an unadulterated overview over organizations' information security investment decisions, evaluations and learning strategies and (2) a comparison of the self-portrayal of firms with regard to their information security investment management with an unbiased external view of consulting firms on this topic. Therefore I obtain genuine information on how security investment is managed in firms. With the requirements raised in this publication, academic researchers can conduct new research on the implementation of decision, evaluation processes and learning strategies that can be supported in firms so that future information security investments become more effective in practice.

In paper 3, I regard timing in two dimensions, namely the time of announcement in relation to the time of investment and the time of announcement in relation to the time of a fundamental security incident. The operational performance of information security investments is assessed by examining the relationship between the investment announcements and their stock market reaction whereby I focus on these two time dimensions. I found out that both dimensions influence the stock market return of the investing organization in terms of organizational performance. In particular: (1) after fundamental security incidents, the stock price will react more positively to a firm's announcement of actual information security investments than to announcements of the intention to invest; (2) the stock price will react more positively to a firm's announcements of the intention to invest after the fundamental security incident compared to before; and (3) the stock price will react more positively to a firm's announcements of actual information security investments after the fundamental security incident compared to before.

Part II

Research Papers

2

Paper 1: A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory

Status:	Published
Conference:	36th International Conference on Information Systems (ICIS 2015)
CORE Ranking:	A*
VHB-Jourqual 3:	A
Full citation:	Weishäupl, E., Yasasin, E., and Schryen, G (2015). A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory. In Carte, T., Heinzl, A., and Urquhart, C., editors, *Proceedings of the Thirty-Sixth International Conference on Information Systems*, pages 1-22, December 13-16, Fort Worth, Texas, USA. Association for Information Systems.
Link:	https://aisel.aisnet.org/icis2015/proceedings/SecurityIS/16/

Abstract: The protection of information technology (IT) has become and is predicted to remain a key economic challenge for organizations. While research on IT security investment is fast growing, it lacks a theoretical basis for structuring research, explaining economic-technological phenomena and guide future research. We address this shortcoming by suggesting a new theoretical model emerging from a multi-theoretical perspective adopting the Resource-Based View and the Organizational Learning Theory. The joint application of these theories allows to conceptualize in one theoretical model the organizational learning effects that occur when the protection of organizational resources through IT security countermeasures develops over time. We use this model of IT security investments to synthesize findings of a large body of literature and to derive research gaps. We also discuss managerial implications of (closing) these gaps by providing practical examples.

Conference Description: *"The annual International Conference on Information Systems (ICIS) is the most prestigious gathering of IS academics and research-oriented practitioners in the world. Billed as the most exclusive AIS conference - and one of the most exclusive in the entire field - ICIS attracts the top research papers in the field, and their authors, from around the world for an invalauble networking and research experience."*

Source: http://aisel.aisnet.org/icis/

3

Paper 2: Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning

Status:	Published
Journal:	Computers & Security
Submitted:	21 August 2017
CORE Ranking:	B
VHB-Jourqual 3:	N/A
Full citation:	Weishäupl, E., Yasasin, E., and Schryen, G. (2017). Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning
Link:	https://www.sciencedirect.com/science/article/pii/S0167404818300555

Abstract: The need to protect resources against attackers is reflected by huge information security investments of firms worldwide. In the presence of budget constraints and a diverse set of assets to protect, organizations have to decide in which IT security measures to invest, how to evaluate those investment decisions, and how to learn from past decisions to optimize future security investment actions. While the academic literature has provided valuable insights into these issues, there is a lack of empirical contributions. To address this lack, we conduct a theory-based exploratory multiple case study. Our case study reveals that (1) firms' investments in information security are largely driven by external environmental and industry-related factors, (2) firms do not implement standardized decision processes, (3) the security process is perceived to impact the business process in a disturbing way, (4) both the implementation of evaluation processes and the application of metrics are hardly existent and (5) learning activities mainly occur at an ad-hoc basis.

Journal Description: *"Computers & Security is the most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world."*

Source: https://www.journals.elsevier.com/computers-and-security/

4

Paper 3: Timing in Information Security: An Event Study on the Impact of Information Security Investment Announcements

Status:	Under Review
Journal:	Computers & Security
Submitted:	7 July 2018
CORE Ranking:	B
VHB-Jourqual 3:	N/A
Full citation:	Szubartowicz, E. and Schryen, G. (2018). Timing in Information Security: An Event Study on the Impact of Information Security Investment Announcements (Under Review)
Link:	https://epub.uni-regensburg.de/37576/
Abstract:	Timing plays a crucial role in the context of information security investments: We regard timing in two dimensions, namely the time of announcement in relation to the time of investment and the time of announcement in relation to the time of a fundamental security incident. The financial value of information security investments is assessed by examining the relationship between the investment announcements and their stock market reaction focusing on the two time dimensions. Using an event study methodology, we found that both dimensions influence the stock market return of the investing organization. In particular: (1) after fundamental security incidents in a given industry, the stock price will react more positively to a firms announcement of actual information security investments than to announcements of the intention to invest; (2) the stock price will react more positively to a firms announcements of the intention to invest after the fundamental security incident compared to before; and (3) the stock price will react more positively to a firms announcements of actual information security investments after the fundamental security incident compared to before. Overall, the lowest abnormal return can be expected when the intention to invest is announced before a fundamental information security incident and the highest return when actual investing after a fundamental information security incident in the respective industry.

Journal Description: *"Computers & Security is the most respected technical journal in the IT security field. With its high-profile editorial board and informative regular features and columns, the journal is essential reading for IT security professionals around the world."*

Source: https://www.journals.elsevier.com/computers-and-security/

5

List of Further Research Papers

During my research, I contributed to further publications which are not directly related to the research questions of this dissertation but may also be interesting for the reader:

- Weishäupl, E. (2017). Towards a Multi-objective Optimization Model to Support Information Security Investment Decision-making. In: *Proceedings of the 4th International Workshop on Security in Highly Connected IT Systems*, June 21-22, 2017, Neuchâtel, Switzerland. FORSEC Research Association.
- Weishäupl, E., Kunz, M., Yasasin, E., Wagner, G., Prester, J., Schryen, G., and Pernul, G. (2015). Towards an Economic Approach to Identity and Access Management Systems Using Decision Theory. In: Pernul, G., Schryen, G., and Schillinger, R., editors, *Proceedings of the Second International Workshop on Security in Highly Connected IT Systems*, September 21-22, Vienna, Austria. FORSEC Research Association.
- Weishäupl, E., Yasasin, E., Schryen, G. (2015). IT Security Investments Through the Lens of the Resource-Based View: A new Theoretical Model and Literature Review. In: Becker, J., vom Brocke, J., and de Marco, M., editors *Proceedings of the Twenty-Third European Conference on Information Systems*, Paper 198, May 26-29, Münster, Germany. Association for Information Systems.
- Reinfelder, L., Weishäupl, E. (2016). A Literature Review on Smartphone Security in Organizations using a new theoretical Model - The Dynamic Security Success Model. In: *Proceedings of the 20th Pacific Asia Conference on Information Systems*, Chiayi, Taiwan, June 27 - July 1, 2016.
- Fischer, A., Kittel, T., Kolosnjaji, B., Lengyel, T., Mandarawi, W., de Meer, H., Mller, T., Protsenko, M., Reiser, H., Taubmann, B., Weishäupl, E. (2015). CloudIDEA: A Malware Defense Architecture for Cloud Data Centers. In: *Lecture Notes in Computer Science*, 9415, Springer.
- Mandarawi, W., Fischer, A., de Meer, H., Weishäupl, E. (2015). QoS-Aware Secure Live Migration of Virtual Machines. In: Pernul, G., Schryen, G., and Schillinger, R., editors, *Proceedings of the Second International Workshop on Security in Highly Connected IT Systems*, September 21-22, Vienna, Austria. FORSEC Research Association.

- Schryen, G., Weishäupl, E. (2015). IT-Sicherheit: Ökonomisch Planen und Bewerten. In: *Managementkompass*, 2, Frankfurt Business Media, Der F.A.Z.-Fachverlag.
- Rakotondravony, N., Taubmann, B., Mandarawi, W., Weishäupl, E., Xu, P., Kolosnjaji, B., Protsenko, M., de Meer, H., Reiser, H. P. (2017). Classifying Malware Attacks in IaaS Cloud Environments. In: *Journal of Cloud Computing*, 6(1), 26.

Part III

Discussion

6

Discussion

This thesis deals with the organizational planning and evaluation of information security investments. In Part I of this work I framed the academic research in this area including my publications in the Cyber Security Investment Framework for Planning and Evaluation based on Rowe and Gallaher (2006). In this chapter I summarize the results and contributions of my publications in the light of the Cyber Security Investment Framework for Planning and Evaluation and of the developed research questions: The first section provides a summary of this thesis. Thereafter, Section 2 presents the limitations of this thesis. In Section 3 the thesis' repercussions in the light of the developed research questions are discussed and implications for academic and practice are drawn.

6.1 Summary

Information security investments are considered a challenging task by practitioners and academics since there is no direct return of investment but intangible returns such as prevented security incidents or improved reputation (Cavusoglu et al., 2004b; Chai et al., 2011). Nevertheless, academic literature has provided a plethora of research articles to examine information security investments concentrating on different aspects (Weishäupl et al., 2015). Therefore, in a first step, I studied the academic literature to provide an overview over existing methods and models for information security investment planning and evaluation. I found out that the literature on information security investments at the organizational level is fragmented and lacks a theoretical basis. The development of a new theoretical model addresses this deficiency and can be used not only for providing a coherent picture of what the literature has found but also for supporting future theoretical developments in this research area. This resource-based learning model on information security investments integrates two complementary theoretical perspectives on information security investments: While the RBV focusses on the mechanisms how investments into information security resources effect the IT business value generation process and organizational performance, the OLT considers the temporal dynamics of these mechanisms by emphasizing the phenomena of organizational development and organizational learning. I have used the integrative model to review the literature on and to condense

existing knowledge on information security investments, to identify research gaps and to formulate research thrusts. This integrated theory has been applied in the case study (Paper 2) in order to understand how information security investment decisions are made and evaluated in firms. The case study surprisingly concluded that organizations do not measure the changes in organizational performance caused by information security investments (Weishäupl et al., 2018). Therefore firms are not able to evaluate the effectiveness and efficiency of their investment decisions and to learn from past decisions to optimize future investment strategies. I address this problem with an event study (Paper 3) examining the organizational performance in terms of stock market returns.

6.2 Limitations

In this section, I discuss the methodological and theoretical limitations of the individual research papers and the thesis. Overall, the most important limitation is the theoretical limitation originated from the theoretical model which serves as a basis for Paper 1 and Paper 2. The theoretical model based on the RBV and the OLT considers key factors in the area of information security investments because with the integrative model, (a) diverse assets such as systems, data or processes, which need to be protected, can be modeled as resources, (b) both tangible and intangible resources, such as firewalls, and security knowledge, can be explicitly considered (Cavusoglu et al., 2015) and (c) the firm's ability to learn and integrate temporal and dynamic feedback loops are taken into account. Both the RBV and the OLT are established theories in the IS literature (Iyengar et al., 2015; Kwon and Johnson, 2014; Wade and Hulland, 2004; Wu et al., 2015) and I consider them an appropriate theoretical basis in the context of information security investments. However, since the integrative model dictates the focus of Paper 1 and Paper 2, I had to exclude some research papers in the literature analysis in Paper 1 (Weishäupl et al., 2015). Moreover, my interview questions during the interviews for Paper 2 had to remain within the boundaries of the theoretical model (Weishäupl et al., 2018).

The limitations of the literature review (Paper 1) are both methodological and theoretical (Weishäupl et al., 2015): To identify relevant studies for the literature review, I followed a precise and structured process. Nevertheless I may have missed some important and pertinent research articles. Moreover, since the theoretical foundation based on the RBV and OLT has boundaries, I had to exclude papers which focus on the technical perspective of information security (e.g., Lyu and Lau (2000)) and papers that do not focus on information security investment (e.g., Moore et al. (2001)).

The limitations of the case study (Paper 2) are both methodological and theoretical (Weishäupl et al., 2018): (1) Having conducted a small-sample case study, I cannot claim a generalization although the study covers a broad variety of different sectors and firm sizes. (2) Consulting firms might have limited insights in the security investment management of their clients. Therefore, future

case studies should also include interviews with these clients and compare results with those of the corresponding consulting firms. (3) The adoption of the multi-theoretical view focuses on information security investments and activities of organizations. Therefore, similar to the literature review, information security phenomena at the individual level, for example learning of individuals, are out of this work's scope.

The limitations of the event study (Paper 3) are methodological and related to the data collected for the analysis: As I gathered the public information security investment announcements from newspaper articles, relevant information could not be included in the analysis: For instance, the amount of investment could not be assessed. However, I assume that the amount of invested capital plays an important role on stock price returns: Investors might reward organizations that spend comparatively large sums with higher abnormal stock price returns than firms investing smaller sums or firms not investing at all. Furthermore, a larger sample size may improve the robustness of the results: Due to the screening process and the requirements on the data, I had to filter out a large portion of the announcements. With 63 information security investment announcements, I regard a relatively small sample size compared to, for instance, Brock and Levy (2013) or Chai et al. (2011).

The limitation of this thesis can be derived from the Cyber Security Investment Framework for Planning and Evaluation based on Rowe and Gallaher (2006): With Paper 1 focusing on the information security drivers and resources influencing information security investment decisions, Paper 2 concentrating on the evaluation of and the learning from those decisions and Paper 3 studying the influence of those decisions on the organizational performance, some aspects of the Cyber Security Investment Framework for Planning and Evaluation based on Rowe and Gallaher (2006) are neglected. In this thesis, I do not study the influence of information security investment decision processes on the cyber security infrastructure and on the nature and frequency of cyber security breaches. Moreover, I do not regard the interrelations of the implementation strategy as part of the cyber security investment decision process with the budget allocation process as depicted in Figure 3 in Section 1 of this thesis. These neglected aspects of organizational information security planning and evaluation were not in the focus of my thesis and therefore need to be examined in detail in the future.

6.3 Repercussions on the Research Questions and Implications for Academic and Practice

In the following, I discuss this thesis' repercussions and implications for academic and practice in the light of the developed research questions:

6.3.1 Research Question 1

Addressing research question 1, I conclude that the influence of single external drivers are examined thoroughly in academic literature (Weishäupl et al., 2015). Nevertheless future research need to pay attention to the interaction between these external drivers: Surprisingly, so far the literature is silent on how the interaction (regarding interdependencies) of different external driver impacts a firm's investment decision disaggregated in technological and human information security resources. As there are multiple coinciding security drivers which influence information security investment decisions in firms, an investigation of the interaction between these drivers is of particular importance to optimize investment strategies. For example, a health care provider must comply with country-specific and health care industry-related regulations (Von Solms and Von Solms, 2004). Compliance to both might lead to interferences and to the question how to unify the different regulations to one optimal investment strategy.

Regarding the information security resources and their influence on the firm's implementation strategy we disaggregated the resources along the two dimensions of technological versus human IT resources, and security versus non security resources in Paper 1 (Weishäupl et al., 2015). It should be noticed that technological and human information resources, with regard to both security and non-security information resources, often need to be complemented in order to be effective (Su, 2006). For example, the investment in a (technological) single sign on (SSO) authentication system also requires maintenance by, e.g., a security engineer, which represents a human information resource (Su, 2006). Unsurprisingly, I conclude that the different information security resources such as firewalls, intrusion detection systems and encryption techniques are sufficiently covered in academic literature. However, the influence of those information security resources on the cyber security investment decision process in particular on the implementation strategy needs to be a topic in future research. Regarding the drivers for information security investments I draw the following conclusion: The literature review revealed that there is a substantial body of literature on the importance of considering external drivers when investing in information security resources (Weishäupl et al., 2015). However, it is yet not understood how these factors interact and jointly affect investment decisions. This issue should be addressed in future work. Understanding these effects is crucial for informing firms on how they should use or even extend their budget when investing in technological and organizational information security resources. Moreover, as discussed in Paper 2, firms revealed an unexpected fact: Regulations which are not directly related to information security can influence information security nonetheless and therefore need to be examined in detail in the future (Weishäupl et al., 2018): The academic literature deals exhaustively with impacts of information security specific laws (Kwon and Johnson, 2014; Ghose and Rajan, 2006; Connolly and Lang, 2013), but it is silent on laws which are not directly related to information security. In particular, under the aspect of internationally operating organizations where data is distributed globally, I recommend to shift these complex legal requirements into focus of future academic research. Unsurprisingly, in real-world organizations

country and industry-specific drivers have the strongest influence on organizational information security investments (Weishäupl et al., 2018). Regarding the information security resources which are differentiated in security, non-security, technological and human resources, I conclude the following: As expected, research on investments in technological and human information security resources is thoroughly and well-examined (Weishäupl et al., 2015). In practice, organizations usually invest in classical information security resources such as firewalls, antivirus-programs and workshops and therefore every company has a basic technical security equipment. This result also meets my expectations. Moreover, firms mainly invest in human security resources including a Chief Information Security Officer (CISO) and his department for information security, external consultants, and workshops for employees to raise awareness. Consistent with the academic literature, I observed that the distinction between security and non-security resources is blurry in practice (Weishäupl et al., 2018). The reason for that is, that for instance a technical security resource like a firewall is managed by the IT department not the IT security department of an organization (Weishäupl et al., 2018). Moreover, it is challenging to distinguish between an IT budget and an information security budget. However, in literature, models and methods often require an IT security budget (Gordon and Loeb, 2002a,b; Mukhopadhyay et al., 2013; Olifer et al., 2017). I hypothesize that models requiring to specify the IT security budget are difficult to apply in organizations. This assumption was backed up by the interview partners in Weishäupl et al. (2018). In the future, academic literature should provide explicit guidelines for the distinction of IT budget and IT security budget.

6.3.2 Research Question 2

Regarding research question 2, I surprisingly found out that organizations are not sufficiently evaluating their information security investment decisions. The case study revealed that contradictory to academic research, metrics like ROSI or NPV are not applied in practice and evaluation processes are not implemented (Weishäupl et al., 2018). The metrics and methods developed by academics are too complex and time consuming for real world application. Moreover, these metrics do not adequately reflect the assumptions and facts in practice. With the exception of banks which are forced by audits, organizations in general do not evaluate their security investments decisions and therefore they can not efficiently use the results of the evaluation to learn for future information security investment decisions (Weishäupl et al., 2018). Regarding the learning from changes in organizational performance to improve future investment decision the following conclusion can be drawn: Consistent with my assumptions, the concept of learning when it comes to information security investments within an organization has received very few attention in existing academic literature (Weishäupl et al., 2015): For instance, Hamdan (2013) refers to learning as part of five major capabilities for future readiness. Wang et al. (2008) propose a value-at-risk (VaR) approach which helps to quantify the risk of information security and can determine proper security solutions based on its risk preference and thus gives insights to learn from the past: The authors state that with the proposed

VaR approach, the firm can find out whether extreme daily losses are influenced by environmental factors and therefore make strategic investment in information security more effective (Wang et al., 2008). However, in practice, understanding these effects is of significant importance due to continuously changing external factors (Williams, 2001). Organizations need to constantly learn from the impact that past information security investments have had on the organizational performance and adapt their long-term strategies and medium-term actions (Weishäupl et al., 2015). The case study revealed that, in practice, from the two existing learning strategies (single and double loop) firms prefer, according to the interviews, single loop learning as a fast reaction to incidents rather than searching for a long lasting rectification. However, learning, whether single or double loop, is always triggered by incidents and not intrinsically motivated (Weishäupl et al., 2018).

6.3.3 Research Question 3

For research question 3, I come to the following conclusion: According to academic research, information security investments can have a positive influence on the stock market value of the investing firm (Bose and Leung, 2013; Brock and Levy, 2013; Chai et al., 2011): Investments in identity theft countermeasures or investments with commercial exploitation result in a positive stock market return (Bose and Leung, 2013; Chai et al., 2011; Xu et al., 2017). Regarding the organizational performance resulting from information security investment decisions I come to the following conclusion: A positive impact of information security investments - in both technological and human resources - on the cyber security infrastructure and the organizational performance of a firm has been identified and measured using different metrics (Weishäupl et al., 2015). We expect that this impact is mediated through its influence on security processes and business processes as there is consensus in the literature that the causal relationship between investments in IT assets in general and the organizational performance shows such mediation effects. For information security investments, these mediation effects are neglected in the literature (Dedrick et al., 2003; Dehning and Richardson, 2002; Melville et al., 2004; Schryen, 2013; Soh and Markus, 1995). Surprisingly, although a plethora of metrics and models to measure changes in organizational performance are developed (Drugescu and Etges, 2006; Pfleeger and Rue, 2008; Su, 2006), they are not applicable in real-world organizations (Weishäupl et al., 2018). Therefore, I measured the changes in organizational performance in terms of the stock market return: Consistent with prior academic studies (Chai et al., 2011; Brock and Levy, 2013; Bose and Leung, 2013; Xu et al., 2017), the results indicate that information security investments can have a positive influence on the stock market value of the investing firm under certain conditions and that the timing of information security investment announcements plays a significant role. However, I observe that information security investments can result in negative stock market return and negative changes in organizational performance: I assume that investors do not recognize the necessity of information security investments, since those investments do not generate direct profit for the organization and therefore investors would prefer investments in more

profitable business sectors instead (Chai et al., 2011). This claim is backed up by academic literature: Information security investments might not improve a firm's stock return (Chai et al., 2011; Dos Santos et al., 1993; Im et al., 2001) because of the investors' negative opinions or doubts about a firm's resource allocation or about its investment priority (Chai et al., 2011).

Regarding the time of information security investments in relation to the investment announcement and to a fundamental security incident in the same industry I conclude that the market reactions for intended and actual information security investment announcements are negative before fundamental security incidents, i.e. the stock market punishes both intended and actual information security investments. This conclusion contradicts my expectations: I assumed that actual information security investment announcements always lead to a positive stock market return. However, after fundamental security incidents, the return for information security investments - whether intended or actual - is positive and notable higher than for announcements before the incident.

Overall, I conclude that the planning and evaluation of information security investments needs to move in the center of attention of both academic researchers and practitioners: I recommend for academic research to concentrate on the real-world applicability of their developed metrics, models and methods. Practitioners should be aware that information security investments are not costs without return but can result in positive stock market return. In the light of increasing information security threats they should adapt their security infrastructure accordingly. I recommend to intensify the collaboration between practitioners and researchers in order to optimize methods for planning and evaluation to prevent future fundamental security incidents.

Part IV

Bibliography

References

Alner, M. (2001). The Effects of Outsourcing on Information Security. *Information Systems Security*, 10(2):1–9.

Anderson, E. E. and Choobineh, J. (2008). Enterprise Information Security Strategies. *Computers & Security*, 27(1):22–29.

Anderson, J. P. (1972). Computer Security Technology Planning Study. Volume 2. Technical report, Anderson (James P) and Co Fort Washington PA.

Anderson, R. (2001). Why Information Security is Hard - An Economic Perspective. In Faigin, D., editor, *Proceedings of the Seventeenth Annual Computer Security Applications Conference*, pages 358–365, December 10-14, New Orleans, Louisiana, USA. IEEE Computer Society.

Anderson, R. and Schneier, B. (2005). Guest Editors' Introduction: Economics of Information Security. *IEEE Security & Privacy*, 3(1):12–13.

Andoh-Baidoo, F. K. and Osei-Bryson, K.-M. (2007). Exploring the Characteristics of Internet Security Breaches that impact the Market Value of Breached Firms. *Expert Systems with Applications*, 32(3):703–725.

Ang, S. and Straub, D. W. (1998). Production and Transaction Economies and IS Outsourcing: A Study of the US Banking Industry. *MIS Quarterly*, 22(4):535–552.

Baker, W. H. and Wallace, L. (2007). Is Information Security under Control?: Investigating Quality in Information Security Management. *IEEE Security & Privacy*, 5(1).

Bandyopadhyay, T., Mookerjee, V. S., and Rao, R. C. (2009). Why IT Managers don't go for Cyber-Insurance Products. *Communications of the ACM*, 52(11):68–73.

Barnard, L. and von Solms, R. (2000). A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Computers & Security*, 19(2):185–194.

Belanger, F., Hiller, J. S., and Smith, W. J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *The journal of strategic Information Systems*, 11(3):245–270.

Beresnevichiene, Y., Pym, D., and Shiu, S. (2010). Decision Support for Systems Security Investment. In *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010*

IEEE/IFIP, pages 118–125. IEEE.

Bistarelli, S., Fioravanti, F., and Peretti, P. (2006). Defense Trees for Economic Evaluation of Security Investments. In *First International Conference on Availability, Reliability and Security (ARES'06)*, pages 8–pp. IEEE.

Bistarelli, S., Fioravanti, F., Peretti, P., and Santini, F. (2012). Evaluation of Complex Security Scenarios Using Defense Trees and Economic Indexes. *Journal of Experimental & Theoretical Artificial Intelligence*, 24(2):161–192.

Bodin, L. D., Gordon, L. A., and Loeb, M. P. (2005). Evaluating Information Security Investments using the Analytic Hierarchy Process. *Communications of the ACM*, 48(2):78–83.

Bodin, L. D., Gordon, L. A., and Loeb, M. P. (2008). Information Security and Risk Management. *Communications of the ACM*, 51(4):64–68.

Böhme, R. (2010). Security Metrics and Security Investment Models. In *International Workshop on Security*, pages 10–24. Springer.

Böhme, R. and Nowey, T. (2008). Economic Security Metrics. In Eusgeld, I., Freiling, F., and Reussner, R., editors, *Dependability Metrics*, pages 176–187. Springer.

Bojanc, R. and Jerman-Blažič, B. (2008). An Economic Modelling Approach to Information Security Risk Management. *International Journal of Information Management*, 28(5):413–422.

Bojanc, R. and Jerman-Blažič, B. (2012). Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija*, 45(6):276–288.

Bose, I. and Leung, A. C. M. (2013). The Impact of Adoption of Identity Theft Countermeasures on Firm Value. *Decision Support Systems*, 55(3):753–763.

Bose, R. and Luo, X. (2014). Investigating Security Investment Impact on Firm Performance. *International Journal of Accounting & Information Management*, 22(3):194–208.

Breier, J. and Hudec, L. (2013). On Selecting Critical Security Controls. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pages 582–588. IEEE.

Brock, L. and Levy, Y. (2013). The Market Value of Information System (IS) Security for e-Banking. *Online Journal of Applied Knowledge Management*, 1(1):1.

Buck, K., Das, P., and Hanf, D. (2008). Applying ROI Analysis to Support SOA Information Security Investment Decisions. In Cooper, H., editor, *Proceedings of the Seventh IEEE Conference on Technologies for Homeland Security*, pages 359–366, May 12-13, Waltham, Massachusetts, USA. IEEE Boston Section.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security*, 11(3):431–448.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. (2004a). Economics of IT Security Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems*, 14:65–75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., and Benbasat, I. (2015). Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment in Information Security Control Resources. *Information & management*, 52(4):385–400.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004b). A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004c). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1):70–104.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1):28–46.

Cavusoglu, H., Raghunathan, S., and Cavusoglu, H. (2009). Configuration of and Interaction between Information Security Technologies: The case of Firewalls and Intrusion Detection Systems. *Information Systems Research*, 20(2):198–217.

Cavusoglu, H., Raghunathan, S., and Yue, W. T. (2008). Decision-theoretic and Game-theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, 25(2):281–304.

Chai, S., Kim, M., and Rao, H. R. (2011). Firms' Information Security Investment Decisions: Stock Market Evidence of Investors' Behavior. *Decision Support Systems*, 50(4):651–661.

Cheng, E. W. and Li, H. (2001). Information Priority-setting for better Resource Allocation using Analytic Hierarchy Process (AHP). *Information Management & Computer Security*, 9(2):61–70.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. (2008). *Performance Measurement Guide for Information Security*. National Institute of Standards and Technology.

Chou, T.-Y., Seng-cho, T. C., and Tzeng, G.-H. (2006). Evaluating IT/IS Investments: A Fuzzy Multi-Criteria Decision Model Approach. *European Journal of Operational Research*, 173(3):1026–1046.

Cohen, F. (2006). *IT Security Governance Guidebook with Security Program Metrics on CD-ROM*. Auerbach Publications, Boston, Massachusetts, USA, 1st edition.

Connolly, L. and Lang, M. (2013). Information Systems Security: The Role of Cultural Aspects in Organizational Settings. In Hedstrm, K. and Dhillon, G., editors, *Proceedings of the Third Workshop on Information Security and Privacy*, Milan, Italy. Association for Information Systems.

Cremonini, M. and Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In *Proceedings of the Fourth Annual Workshop on the Economics of Information Security*, Cambridge, MA, USA. Harvard University.

Crume, J. (2000). *Inside Internet Security: What Hackers don't want you to know*. Pearson Education.

Daneva, M. (2006). Applying real Options Thinking to Information Security in Networked Organizations.

D'arcy, J. and Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings. *European Journal of Information Systems*, 20(6):643–658.

Debar, H. and Viinikka, J. (2005). Intrusion Detection: Introduction to Intrusion Detection and Security Information Management. *Foundations of security analysis and design III*, pages 207–236.

Dedrick, J., Gurbaxani, V., and Kraemer, K. L. (2003). Information Technology and Economic Performance: A Critical Review of the Empirical Evidence. *ACM Computing Surveys*, 35(1):1–28.

Dehning, B. and Richardson, V. J. (2002). Returns on Investments in Information Technology: A Research Synthesis. *Journal of Information Systems*, 16(1):7–30.

Dos Santos, B. L., Peffers, K., and Mauer, D. C. (1993). The Impact of Information Technology Investment Announcements on the Market Value of the Firm. *Information Systems Research*, 4(1):1–23.

Drugescu, C. and Etges, R. (2006). Maximizing the Return on Investment on Information Security Programs: Program Governance and Metrics. *Information systems security*, 15(6):30–40.

Dutta, A. and McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1):67–87.

Eisenga, A., Jones, T. L., and Rodriguez, W. (2012). Investing in IT Security: How to Determine the Maximum Threshold. *International Journal of Information Security and Privacy*, 6(3):75–87.

Ekelhart, A., Fenz, S., and Neubauer, T. (2009). AURUM: A Framework for. Information Security Risk Management. In Sprague, R. H. S., editor, *Proceedings of the Forty-Second Hawaii International Conference on System Sciences*, pages 1–10, Big Island, HI, USA. IEEE Computer Society.

Ernest Chang, S. and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3):345–361.

Fenz, S., Ekelhart, A., and Neubauer, T. (2011). Information Security Risk Management: In which Security Solutions is it worth investing? *CAIS*, 28:22.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., and Toval, A. (2013). Security and Privacy in Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics*, 46(3):541–562.

Fink, D. (1994). A Security Framework for Information Systems Outsourcing. *Information Management & Computer Security*, 2(4):3–8.

Finne, T. (1998). Special Feature: A Conceptual Framework for Information Security Management. *Computers and Security*, 17(4):303–307.

Forbes, Inc. (2016). Cyber Crime Costs Projected To Reach 2 Trillion Dollar by 2019.

Franqueira, V. N. L., Houmb, S. H., and Daneva, M. (2010). Using Real Option Thinking to Improve Decision Making in Security Investment. *Lecture Notes in Computer Science 6426*, pages 619 – 638.

Gal-Or, E. and Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2):186–208.

Gartner, Inc. (2017). Gartner Predicts Information Security Spending To Reach $93 Billion In 2018. http://www.gartner.com/newsroom/id/3784965. Retrieved: November 10, 2017.

Ghose, A. and Rajan, U. (2006). The Economic Impact of Regulatory Information Disclosure on Information Security Investments, Competition, and Social Welfare. In Anderson, R., editor, *Proceedings of the Fifth Annual Workshop on the Economics of Information Security*, Cambridge, England, UK. University of Cambridge.

Glaspie, H. W. and Karwowski, W. (2017). Human Factors in Information Security Culture: A Literature Review. In *International Conference on Applied Human Factors and Ergonomics*, pages 269–280. Springer.

Glisson, W. B. and Welland, R. (2014). Web Engineering Security (WES) Methodology. *Communications of the Association for Information Systems*, 34(1):1359–1396.

Goel, S. and Shawky, H. A. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, 46(7):404–410.

Goodman, S. E. and Ramer, R. (2007). Global Sourcing of IT Services and Information Security: Prudence before Playing. *Communications of the Association for Information Systems*, 20(1):812–823.

Gordon, L. A. and Loeb, M. P. (2002a). Return on Information Security Investments: Myths vs. Realities. *Strategic Finance*, 84(1):26–31.

Gordon, L. A. and Loeb, M. P. (2002b). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438–457.

Gordon, L. A. and Loeb, M. P. (2006a). Budgeting Process for Information Security Expenditures. *Communications of the ACM*, 49(1):121–125.

Gordon, L. a. and Loeb, M. P. (2006b). Economic Aspects of Information Security: An Emerging Field of Research. *Information Systems Frontiers*, 8(5):335–337.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy*, 22(6):461–485.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, 6(1):24.

Goyal, P., Batra, S., and Singh, A. (2010). A Literature Review of Security Attack in Mobile ad-hoc Networks. *International Journal of Computer Applications*, 9(12):11–15.

Grant, R. M. (1991). The Resource-based Theory of Competitive Advantage: Implications for Strategy Formulation. *California Management Review*, 33(3):114–135.

Grossklags, J., Christin, N., and Chuang, J. (2008). Secure or Insure?: A Game-Theoretic Analysis of Information Security Games. In Huai, J., Chen, R., Hon, H.-W., and Liu, Y., editors, *Proceedings of the Seventeenth International Conference on World Wide Web*, pages 209–218, April 21-25, Beijing, China. Association for Computing Machinery.

Gupta, J. N. (2008). *Handbook of Research on Information Security and Assurance*. IGI Global.

Gupta, M., Chaturvedi, A., and Mehta, S. (2011). Economic Analysis of Tradeoffs between Security and Disaster Recovery. *Communications of the Association for Information Systems*, 28(1):1–17.

Hall, J. H., Sarkani, S., and Mazzuchi, T. A. (2011). Impacts of Organizational Capabilities in Information Security. *Information Management & Computer Security*, 19(3):155–176.

Hamdan, B. J. (2013). Evaluating the Performance of Information Security: A Balanced Scorecard Approach. In *Proceedings of the 10th Southern Association for Information Systems (SAIS 2013)*, volume 11.

Hausken, K. (2006). Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers*, 8(5):338–349.

Hoo, K. J. S. (2000). *How Much Is Enough? A Risk Management Approach to Computer Security*. PhD thesis, Stanford University.

Hooper, E. (2009). Intelligent Strategies and Techniques for Effective Cyber Security, Infrastructure Protection and Privacy. In *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, pages 1–7. IEEE.

Hovav, A., Andoh-Baidoo, F. K., and Dhillion, G. (2007). Classification of Security Breaches and their Impact on the Market Value of Firms. In *Proceedings of the 6th Annual Security Conference*.

Huang, C. D. and Behara, R. S. (2013). Economics of Information Security Investment in the Case of Concurrent Heterogeneous Attacks with Budget Constraints. *International Journal of Production Economics*, 141(1):255–268.

Huang, C. D., Behara, R. S., and Goo, J. (2014). Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis. *Decision Support Systems*, 61:1–11.

Huang, C. D., Hu, Q., and Behara, R. S. (2006). Economics of Information Security Investment in the Case of Simultaneous Attacks. In *WEIS*.

Huang, C. D., Hu, Q., and Behara, R. S. (2008). An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm. *International Journal of Production Economics*, 114(2):793–804.

Hui, K.-L., Hui, W., and Yue, W. T. (2012). Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. *Journal of Management Information Systems*, 29(3):117–156.

Im, K. S., Dow, K. E., and Grover, V. (2001). A Reexamination of IT Investment and the Market Value of the FirmAn Event Study Methodology. *Information systems research*, 12(1):103–117.

Iyengar, K., Sweeney, J. R., and Montealegre, R. (2015). Information Technology Use as a Learning Mechanism: The Impact of IT Use on Knowledge Transfer Effectiveness, Absorptive Capacity, and Franchisee Performance. *MIS Quarterly*, 39(3):615–641.

Jakoubi, S., Neubauer, T., and Tjoa, S. (2009). A Roadmap to Risk-Aware Business Process Management. In Hai, J. and Zhang, L.-J., editors, *Proceedings of the 5th IEEE Asia-Pacific Services Computing Conference*, pages 23–27, Singapore, Singapore. IEEE Computer Society.

Jing, L. (2009). Risk Evaluation Process Model of Information Security. In *International Conference on Measuring Technology and Mechatronics Automation*, pages 321–324.

Johnson, A. M. (2009). Business and Security Executives Views of Information Security Investment Drivers: Results from a Delphi Study. *Journal of Information Privacy and Security*, 5(1):3–27.

Johnston, A. C. and Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM*, 52(1):126–129.

Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International journal of information management*, 23(2):139–154.

Karlsson, F., Karlsson, F., Kolkowska, E., Kolkowska, E., Prenkert, F., and Prenkert, F. (2016). Inter-Organisational Information Security: A Systematic Literature Review. *Information & Computer Security*, 24(5):418–451.

Khalfan, A. M. (2004). Information Security Considerations in IS/IT Outsourcing Projects: A Descriptive Case Study of Two Sectors. *International Journal of Information Management*, 24(1):29–42.

Khansa, L. and Liginlal, D. (2009). Valuing the Flexibility of Investing in Security Process Innovations. *European Journal of Operational Research*, 192(1):216–235.

Kiely, M., Kobe, E., MacArthur, A., Polk, M., Rains, E., Andrijcic, E., Crawford, J., and Horowitz, B. (2006). Macro-Economic Cyber Security Models. In *IEEE Systems and Information Engineering Design Symposium*, pages 284–291. IEEE.

Knapp, K. J., Morris, R. F., Marshall, T. E., and Byrd, T. A. (2009). Information Security Policy: An Organizational-Level Process Model. *Computers & Security*, 28(7):493–508.

Kraemer, S. and Carayon, P. (2007). Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists. *Applied ergonomics*, 38(2):143–154.

Kraemer, S., Carayon, P., and Clem, J. (2009). Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. *Computers & security*, 28(7):509–520.

Kruger, H. A. and Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness. *computers & security*, 25(4):289–296.

Kumar, R. L., Park, S., and Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. *Journal of Management Information Systems*, 25(2):241–280.

Kwon, J. and Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, 38(2):451–471.

Laudon, K. C. and Laudon, J. P. (2015). *Management Information Systems: Managing the Digital Firm Plus MyMISLab with Pearson eText–Access Card Package*. Prentice Hall Press.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., and Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. In *Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS 2013)*, pages 2978–2987.

Lee, Y. J., Kauffman, R. J., and Sougstad, R. (2011). Profit-maximizing Firm Investments in Customer Information Security. *Decision Support Systems*, 51(4):904–920.

Liu, W., Tanaka, H., and Matsuura, K. (2008). Empirical-analysis Methodology for Information-Security Investment and its Application to reliable Survey of Japanese Firms. *Information and Media Technologies*, 3(2):464–478.

Ljungdahl, M. and Nordström, M. (2016). Security Analysis of Machine Monitoring Sensor Communication.

Locher, C. (2005). Methodologies for Evaluating Information Security. Investments - What Basel II Can Change in the Financial Industry. In Dieter Bartmann, Federico Rajola, J. K. D. E. A. R. W. P. E.-D. J. B. F. B. C. W., editor, *Proceedings of the Thirteenth European Conference on Information Systems*, Regensburg, Germany. Association of Information Systems.

Lyu, M. R. and Lau, L. K. (2000). Firewall Security: Policies, Testing and Performance Evaluation. In *Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International*, pages 116–121. IEEE.

Malandrin, L. J. A. A. and Carvalho, T. C. (2013). Maintaining Information Security in the New Technological Scenario. *Pacific Asia Journal of the Association for Information Systems*, 5(3):43–64.

Matsuura, K. (2009). Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. In *Managing Information Risk and the Economics of security*, pages 99–119. Springer.

Melville, N., Kraemer, K., and Gurbaxani, V. (2004). Review: Information Technology and Organizational Performance: An Integrative Model of IT Business Value. *MIS Quarterly*, 28(2):283–322.

Moore, A. P., Ellison, R. J., and Linger, R. C. (2001). Attack Modeling for Information Security and Survivability. Technical report, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2013). Cyber-Risk Decision Models: To Insure IT or Not? *Decision Support Systems*, 56:11–26.

Olifer, D., Goranin, N., Kaceniauskas, A., and Cenys, A. (2017). Controls-Based Approach for Evaluation of Information Security Standards Implementation Costs. *Technological and Economic Development of Economy*, 23(1):196–219.

Peteraf, M. A. (1993). The Cornerstones of Competitive Advantage: A Resource-based View. *Strategic Management Journal*, 14(3):179–191.

Pfleeger, S. L. and Rue, R. (2008). Cybersecurity Economic Issues: Clearing the path to good Practice. *IEEE software*, 25(1).

Purser, S. A. (2004). Improving the ROI of the Security Management Process. *Computers & Security*, 23(7):542–546.

Quaye, S. J. and Harper, S. R. (2014). *Student Engagement in Higher Education: Theoretical Perspectives and Practical Approaches for diverse Populations*. Routledge.

Rees, J., Bandyopadhyay, S., and Spafford, E. H. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM*, 46(7):101–106.

Reniers, G. and Soudan, K. (2010). A Game-Theoretical Approach for Reciprocal Security-Related Prevention Investment Decisions. *Reliability Engineering & System Safety*, 95(1):1–9.

Rowe, B. R. (2007). Will Outsourcing IT Security Lead to a Higher Social Level of Security? In *Workshop on the Economics of Information Security 2007 (WEIS 2007)*.

Rowe, B. R. and Gallaher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. In Anderson, R., editor, *Proceedings of the Fifth Workshop on the Economics of Information Security*, pages 1–23, June 26-28, Cambridge, England, United Kingdom. Robinson College.

Safa, N. S., Von Solms, R., and Futcher, L. (2016). Human Aspects of Information Security in Organisations. *Computer Fraud & Security*, 2016(2):15–18.

Salisbury, W. D., Ferratt, T. W., and Wynn Jr, D. (2015). Issues and Opinions: Assessing the Emphasis on Information Security in the Systems Analysis and Design Course. *Communications of the Association for Information Systems*, 36(18):337–356.

Sawik, T. (2013). Selection of Optimal Countermeasure Portfolio in IT Security Planning. *Decision Support Systems*, 55(1):156–164.

Schatz, D. and Bashroush, R. (2017). Economic Valuation for Information Security Investment: A systematic Literature Review. *Information Systems Frontiers*, 19(5):1205–1228.

Schryen, G. (2013). Revisiting IS Business Value Research: What we already know, What we still need to know, and How we can get there. *European Journal of Information Systems*, 22(2):139–169.

Shane, S. (1994). The Effect of National Culture on the Choice Between Licensing and Foreign Direct Investment. *Strategic Management Journal*, 15(8):627–642.

Sheen, J. (2010). Fuzzy Economic Decision-Models for Information Security Investment. In *Proceedings of the Ninth WSEAS International Conference on Instrumentation, Measurement, Circuits and Systems*, pages 141–147, Hangzhou, China. Association for Computing Machinery.

Silic, M., Back, A., and Silic, D. (2015). Taxonomy of Technological Risks of Open Source Software in the Enterprise Adoption Context. *Information & Computer Security*, 23(5):570–583.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49(8):97–100.

Soh, C. and Markus, M. L. (1995). How IT Creates Business Value: A Process Theory Synthesis. In Ariav, G., Beath, C., DeGross, J. I., Hoyer, R., and Kemerer, C. F., editors, *Proceedings of the Sixteenth International Conference on Information Systems*, pages 29–41, December 10-13, Amsterdam, The Netherlands. Association for Information Systems.

Sonnenreich, W., Albanese, J., Stout, B., et al. (2006). Return on Security Investment (ROSI)-A practical Quantitative Model. *Journal of Research and practice in Information Technology*, 38(1):45.

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016). Information Security Management Needs More Holistic Approach: A Literature Review. *International Journal of Information Management*, 36(2):215–225.

Spagnoletti, P. and Resca, A. (2008). The Duality of Information Security Management: Fighting against Predictable and Unpredictable Threats. *Journal of Information System Security*, 4(3):46–62.

Spencer, P. R. (2000). Valuing Information Assets for Security Risk Management. *Information Systems Security, Auerbach Publications*, 9(4).

Srinidhi, B., Yan, J., and Tayi, G. K. (2015). Allocation of Resources to Cyber-security: The Effect of Misalignment of Interest between Managers and Investors. *Decision Support Systems*, 75:49–62.

Stoneburner, G., Goguen, A. Y., and Feringa, A. (2002). Sp 800-30. Risk Management Guide for Information Technology Systems.

Straub, D. W. and Welke, R. J. (1998). Coping with Systems risk: Security Planning Models for Management Decision Making. *MIS quarterly*, pages 441–469.

Su, X. (2006). *An Overview of Economic Approaches to Information Security Management*. Centre for Telematics and Information Technology, University of Twente.

Sumner, M. (2009). Information Security Threats: A comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, 26(1):2–12.

Tanaka, H., Matsuura, K., and Sudoh, O. (2005). Vulnerability and Information Security Investment: An Empirical Analysis of e-local Government in Japan. *Journal of Accounting and Public Policy*, 24(1):37–59.

Tatsumi, K.-i. and Goto, M. (2010). Optimal timing of information security investment: A real options approach. In *Economics of Information Security and Privacy*, pages 211–228. Springer.

Van Niekerk, J. F. (2010). *Fostering Information Security Culture through Intergrating Theory and Technology*. PhD thesis, Nelson Mandela Metropolitan University.

Von Solms, B. and Von Solms, R. (2004). The 10 Deadly Sins of Information Security Management. *Computers & Security*, 23(5):371–376.

Vroom, C. and von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computers & Security*, 23(3):191–198.

Vuorinen, J. and Tetri, P. (2012). The Order Machine-The Ontology of Information Security. *Journal of the Association for Information Systems*, 13(9):695–713.

Wade, M. and Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, 28(1):107–142.

Wang, J., Chaudhury, A., and Rao, H. R. (2008). A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, 19(1):106–120.

Wang, S.-L., Chen, J.-D., Stirpe, P. A., and Hong, T.-P. (2011). Risk-Neutral Evaluation of Information Security Investment on Data Centers. *Journal of Intelligent Information Systems*, 36(3):329–345.

Wawrzyniak, D. (2006). Information Security Risk Assessment Model for Risk Management. In Simone Fischer-Hbner, Stevel Furnell, C. L., editor, *Proceedings of the Third international Conference on Trust, Privacy, and Security in Digital Business*, pages 21–30. Springer, Wroclaw, Poland.

Weishäupl, E. (2017). Towards a Multi-objective Optimization Model to Support Information Security Investment Decision-making. In *Proceedings of the 4th Workshop on Security in Highly Connected IT Systems*, pages 37–42. ACM.

Weishäupl, E., Yasasin, E., and Schryen, G. (2015). A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory.

Weishäupl, E., Yasasin, E., and Schryen, G. (2018). Information security investments: an exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*.

Werlinger, R., Hawkey, K., and Beznosov, K. (2009). An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management. *Information Management & Computer Security*, 17(1):4–19.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, 46(8):91–95.

Willemson, J. (2006). On the Gordon Loeb Model for Information Security Investment. In *WEIS*.

Williams, P. (2001). Information Security Governance. *Information Security Technical Report*, 6(3):60–70.

Wood, C. C. and Parker, D. B. (2004). Why ROI and Similar Financial Tools are not advisable for Evaluating the Merits of Security Projects. *Computer Fraud & Security*, 2004(5):8–10.

Wu, S. P.-J., Straub, D. W., and Liang, T.-P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers. *MIS Quarterly*, 39(2):497–518.

Xu, F., Luo, X. R., Zhang, H., Liu, S., and Huang, W. W. (2017). Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect. *Information Systems Frontiers*, pages 1–15. In Press.

Yeo, M. L., Rolland, E., Ulmer, J. R., and Patterson, R. A. (2014). Risk Mitigation Decisions for IT Security. *ACM Transactions on Management Information Systems (TMIS)*, 5(1):5.

Yu, S., Doss, R., Zhou, W., and Guo, S. (2013). A General Cloud Firewall Framework with Dynamic Resource Allocation. In *Communications (ICC), 2013 IEEE International Conference on*, pages 1941–1945. IEEE.